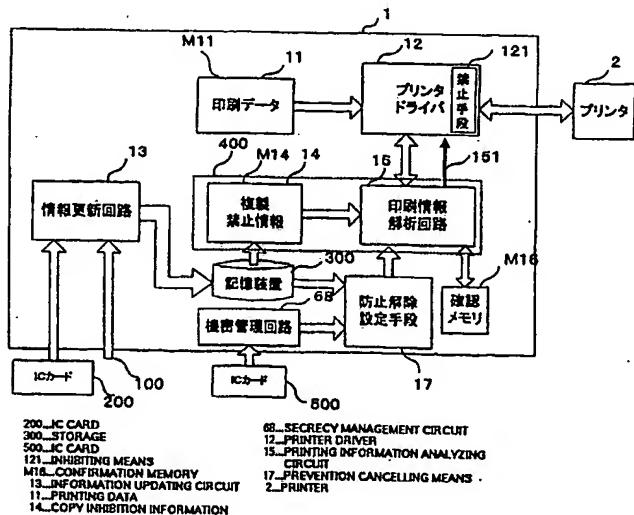




(51) 国際特許分類7 H04N 1/40, 1/387		A1	(11) 国際公開番号 WO00/51338					
			(43) 国際公開日 2000年8月31日(31.08.00)					
<p>(21) 国際出願番号 PCT/JP00/01097</p> <p>(22) 国際出願日 2000年2月25日(25.02.00)</p> <p>(30) 優先権データ</p> <table> <tr> <td>特願平11/49996</td> <td>1999年2月26日(26.02.99)</td> <td>JP</td> </tr> <tr> <td>特願平11/49997</td> <td>1999年2月26日(26.02.99)</td> <td>JP</td> </tr> </table> <p>(71) 出願人 (米国を除くすべての指定国について) 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP] 〒571-0050 大阪府門真市大字門真1006番地 Osaka, (JP)</p> <p>(72) 発明者 ; および</p> <p>(75) 発明者／出願人 (米国についてのみ) 小嶋章夫(KOJIMA, Akio)[JP/JP] 〒572-0039 大阪府寝屋川市池田3-9-7-205 Osaka, (JP)</p> <p>桑原康浩(KUWAHARA, Yasuhiro)[JP/JP] 〒570-0003 大阪府守口市大日町3-32-11-603 Osaka, (JP)</p> <p>渡辺辰巳(WATANABE, Tatsumi)[JP/JP] 〒619-0232 京都府相楽郡精華町桜ヶ丘3-32-8 エルミネンス桜ヶ丘101 Kyoto, (JP)</p>		特願平11/49996	1999年2月26日(26.02.99)	JP	特願平11/49997	1999年2月26日(26.02.99)	JP	(74) 代理人 福井豊明(FUKUI, Toyoaki) 〒540-0026 大阪府大阪市中央区内本町2丁目1番19号 内本町松屋ビル10 860号 福井特許事務所 Osaka, (JP)
特願平11/49996	1999年2月26日(26.02.99)	JP						
特願平11/49997	1999年2月26日(26.02.99)	JP						
		(81) 指定国 JP, US	添付公開書類 国際調査報告書					

(54)Title: DATA MONITORING METHOD, DATA MONITORING DEVICE, COPYING DEVICE, AND STORAGE MEDIUM

(54)発明の名称 データ監視方法、データ監視装置、複製装置および記憶媒体



(57) Abstract

Each copy element of data being an object to be monitored such as printing data or reading data including at least one kind of copy elements is monitored according to at least one kind of copy inhibition information stored in inhibition information storage means and capable of being updated. By the monitoring, when one of the copy elements is judged to agree with the kind of copy inhibition information, input or output of the data being monitored is inhibited. Secrecy management information is given to the copy inhibition information, and a secrecy management level of a user is assigned to each user. In such a way, when the secrecy management level is higher than that of the secrecy management information, the inhibition of the input or output is canceled. An ID for tracing a device which has copied a printed matter is given to the copied printed matter so as to prevent unauthorized copies from diffusing.

(57)要約

禁止情報記憶手段に収容されるとともに更新可能な少なくとも1種の複製禁止情報に基づいて、少なくとも1種の複製要素より構成される印刷データ、閲覧データ等の監視対象データの各複製要素を監視しておき、この監視処理によって、前記各複製要素が前記複製禁止情報の1種と一致すると見なされたときに監視対象データの入力または出力を禁止する。前記複製禁止情報情報に機密管理情報を与える一方で、各ユーザに機密管理レベルを与えておく。これによって、ユーザの機密管理レベルが前記機密管理情報のレベルより高いときには、上記入力あるいは出力の禁止を解除する。更に、複製された印刷物に当該印刷物が複製された装置を追跡できるIDを含ませて、不正複製の拡散を防止できる。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE アラブ首長国連邦	DM ドミニカ	KZ カザフスタン	RU ロシア
AG アンティグア・バーブーダ	DZ アルジェリア	LC セントルシア	SD スーダン
AL アルバニア	EE エストニア	LI リヒテンシュタイン	SE スウェーデン
AM アルメニア	ES スペイン	LK スリ・ランカ	SG シンガポール
AT オーストリア	FI フィンランド	LR リベリア	SI スロヴェニア
AU オーストラリア	FR フランス	LS レソト	SK スロバキア
AZ アゼルバイジャン	GA ガボン	LT リトアニア	SN セネガル
BA ボスニア・ヘルツェゴビナ	GB 英国	LU ルクセンブルク	SZ スワジランド
BB バルバドス	GD グレナダ	LV ラトヴィア	TD チャード
BE ベルギー	GE グルジア	MA モロッコ	TG トガ
BF ブルガリア・ファーン	GH ガーナ	MC モナコ	TJ タジキスタン
BG ブルガリア	GM ガンビア	MD モルドヴァ	TM トルクメニスタン
BJ ベナン	GN ギニア	MG マダガスカル	TR トルコ
BR ブラジル	GR ギリシャ	MK マケドニア旧ユーゴスラヴィア	TT トリニダード・トバゴ
BY ベラルーシ	GW ギニア・ビサオ	共和国	TZ タンザニア
CA カナダ	HR クロアチア	ML マリ	UA ウクライナ
CF 中央アフリカ	HU ハンガリー	MN モンゴル	UG ウガンダ
CG コンゴ	ID インドネシア	MR モーリタニア	US 米国
CH スイス	IE アイルランド	MW マラウイ	UZ ウズベキスタン
CI コートジボアール	IL イスラエル	MX メキシコ	VN ベトナム
CM カメルーン	IN インド	MZ モザンビーク	YU ユーゴースラヴィア
CN 中国	IS アイスランド	NE ニジエール	ZA 南アフリカ共和国
CR コスタ・リカ	IT イタリア	NL オランダ	ZW ジンバブエ
CU キューバ	JP 日本	NO ノールウェー	
CY キプロス	KE ケニア	NZ ニュージーランド	
CZ チェコ	KG キルギスタン	PL ポーランド	
DE ドイツ	KP 北朝鮮	PT ポルトガル	
DK デンマーク	KR 韓国	RO ルーマニア	

明細書

データ監視方法、データ監視装置、複製装置および記憶媒体

5 技術分野

本発明は、複製が禁止された文書・画像データの、不正な複製を防止するデータ監視方法、及びその装置に関するものである。

背景技術

10 近年、ネットワーク化、デジタル化の進展によって、個々の機器がネットワークに接続されて、電子データを手軽に取得、印刷できるようになってきた。一方、DTP (Desktop Publishing) では作成原稿データに忠実な画像形成を目的として技術開発が進められた結果、高精細な複製物が得られるようになってきた。これによって、電子データを取得し、高精細な印刷が簡単にできる環境が整いつつある。

一方で機密管理された文書に対しては複製されると機密漏洩等が問題になる。また、オリジナル原稿と区別がつかない複製物が簡単に得られると、著作物の不正使用、さらには、紙幣や有価証券などの偽造に悪用される恐れがあり、被害が大きい。

20 従来より、カラー複写機には紙幣等に対し偽造防止機能が搭載されていた。第18図は従来のカラー複写機のブロック図である。第18図において、スキャナ110から読み込まれた画像信号は、特定画像判定回路120によって複写が禁止されている紙幣や証券類の画像信号かどうかを画像特徴より判別し、複写が禁止されている場合には縮小画像、鏡像反転などの変換処理を行ってから画像を再生する等の処理をする複写防止機能を起動するようになっている。このような処

理がなされた画像データをプリンタ 130 に出力するようになっているので、複製された画像は容易に偽造物であることが見分けられるようになっている（例えば、特開平 1-316783、特開平 11-275352、特開平 11-355562 の画像処理装置）。

5 近年の傾向として紙の原稿だけでなく、電子データのままで受け渡しされる文書・画像の量も膨大な量になっている。パーソナルコンピュータによって、ネットワーク上から簡単に機密電子文書、著作物データを入手し、高速プリンタで大量に不正印刷できるという課題がある。

ところで、前記先行技術は、スキャナから読み取られた原稿の画像を判別する
10 ものであるので、スキャナから読み取られない電子データに係る前記課題には対処できない。

また、前記従来の技術は紙幣等、その偽造が著しく社会的影響が大きい、極めて限定された範囲での複製の禁止しかできなかつた。ところが特定の事業所を例にとつても、機密を保持すべき電子データは種々あり、その内容は紙幣のように
15 長時間に渡つて一定ではなく、時間経過とともに変化するのが通常である。

ところが、前記従来の技術では複製禁止情報を環境に応じて自由に更新することは困難である。

更に、前記のように文書が電子データに置き代わるにつれて、事業所内の特定の機密文書もサーバに収容されることが多くなり、これらの機密文書を不特定の者が、印刷物としてあるいは単にディスプレイに表示して複製、閲覧することが可能となっている。これらの機密文書は複製、閲覧する権利のある人、ない人があり、その範囲は文書の種類によって異なつてゐる。すなわち文書等に機密管理レベルがあり、ある特定の人に与えられた管理レベルが上記文書等のもつ管理レベルより上である場合にのみ当該文書の複製、閲覧を許可する必要があが、従来の御術では電子データの機密管理レベルまで考慮にいれた複製、閲覧の管理はで
20
25

きない。

本発明は、前記課題を解決するもので、複製が禁止された電子データの不正な複製を未然に、かつ迅速に防止するデータ監視方法およびシステムを提供することを目的とする。

5 また、環境に応じて複製、閲覧の禁止にかかる複製禁止情報の更新が自在なデータ監視方法およびシステムを提供することを目的とする。

更に、電子データの機密管理レベルに応じて複製の禁止あるいは許可の選択が自由にできるデータ監視方法およびシステムを提供することを目的とする。

10 発明の開示

本発明は上記目低を達成するために、以下の手段を採用している。すなわち、本発明は、まず、禁止情報記憶手段に収容されるとともに更新可能な少なくとも1種の複製禁止情報に基づいて、監視手段が、少なくとも1種の複製要素より構成される監視対象データの各複製要素を監視するようにしておく。次いで禁止手段が、前記監視手段による監視処理によって、前記各複製要素が前記複製禁止情報の1種と一致すると見なされたときに監視対象データの入力または出力を禁止する。これによって、複製禁止情報と一致する印刷データ等の監視対象データの複製・閲覧が禁止されることになる。

上記、複製禁止情報は更新手段を用いて、更新することが可能である。更新は20 更新権限のあるユーザが更新できるようにするのが好ましい。また、前記更新は可搬記憶メディアあるいは、ネットワークを介して新しい複製禁止情報を得ることによって実行することができる。

前記更新時に、更新履歴を記憶手段に保存しておいて、当該履歴情報に基づいて更新しようとする複製禁止情報が最新の情報である場合にのみ更新を実行する25 ことが望ましい。

前記複製禁止情報に加えて各複製禁止情報に対応する機密管理情報を禁止情報記憶手段に記憶しておき、当該機密管理情報とユーザの持つ機密管理レベルに基づいて複製禁止、禁止解除を制御するようとする。これによって、複製・閲覧を禁止する必要のないときには、その機能を作用させないことができる。

5 上記複製禁止情報情報はネットワーク上のサーバ装置（マスタ情報記憶手段）に集約して記憶しておくことで、複製禁止処理をする各機器は当該サーバをアクセスするのみで複製禁止情報を得ることができる。ここで上記のように当該サーバ装置より可搬記憶媒体を介して各機器に複製禁止情報を移してもよいし、ネットワークを介して転送してもよい。当該サーバ装置には上記複製禁止情報に加えて各複製禁止情報に対応した機密管理情報を収容することが可能である。

10 本発明では、前記のように印刷データあるいは、閲覧データの複製を禁止するだけでなく、複製された印刷物を生成した機器を追跡することが可能である。すなわち、第1の特定情報抽出手段で監視対象データの生成に関与した所定の装置に固有な識別情報を抽出し、る情報付加手段で、前記監視対象データに前記識別情報をして新たな複製データを生成するようする。

15 前記識別情報は、中央処理装置（CPU）に付与されたチップ識別情報、装置に付与されたIPアドレス等が考えられる。

また、第2の特定情報抽出手段で、複製監視対象データの生成に関与したソフトウェアに固有な特定アプリケーション情報を抽出しておき、情報付加手段で、前記監視対象データに前記特定アプリケーション情報を付与して新たな複製データを生成する。前記特定アプリケーション情報は、ユーザが設定しているメールアドレスを用いるのが効果的である。

20 外部機器より監視対象データを受け入れ、当該監視対象データに従って複製物を生成する複製装置においては、以下のようにすると複製物の追跡ができる。すなわち、抽出手段において、前記監視対象データを解析し、該監視対象データに

関与した所定の装置を特定する固有情報を抽出し、特定情報付与手段で、前記抽出された固有情報を前記監視対象データに付与するようとする。

前記固有情報としては、パーソナルコンピュータを特定できる識別番号、装置に付与されたIPアドレスとすると有益である。

5 また、抽出手段が、前記複製データを解析し、複製データに関与したソフトウェアを特定する固有情報を抽出するようにし、特定情報付与手段が前記抽出された固有情報を新たな複製データとして複製物に付与するようにしてもよい。

図面の簡単な説明

10 第1図は、本発明の第1の実施の形態のパーソナルコンピュータのブロック図

第2図は、本発明の第1の実施の形態のパーソナルコンピュータの使用環境の構成図

第3図は、本発明の第1の実施の形態の複製禁止情報を示した図

第4図は、本発明の第1の実施の形態の印刷情報解析回路のブロック図

15 第5図は、本発明の第2の実施の形態のプリンタのブロック図

第6図は、本発明の第2の実施の形態の印刷情報解析回路のブロック図

第7図は、本発明の第3の実施の形態のネットワークスキャナのブロック図

第8図は、本発明の第4の実施の形態のネットワークプリンタのブロック図

第9図は、本発明の第5の実施の形態のネットワーク上に接続された機器への登録機能説明図

20 第10図は、本発明の第5の実施の形態の複製禁止情報登録装置のブロック図

第11図は、本発明の第6の実施の形態の防止解除設定回路の説明図

第12図は、本発明の第7の実施の形態を示す図

25 第13図は、本発明の第7の実施の形態に使用する機密管理情報のテーブルを示す図

第14図は、本発明の第8の実施の形態のパーソナルコンピュータのブロック図

第15図は、本発明の第9の実施の形態のプリンタのブロック図

第16図は、本発明の第9の実施の形態の印刷結果を示す図
5 第17図は、本発明の第10の実施の形態のネットワークプリンタのブロック図

第18図は、従来のカラー複写機のブロック図

発明を実施するための最良の形態

10 以下、本発明の実施の形態について図面を参照しながら説明する。尚、以下の説明において、複製とは所定のデータ（対象データ）に基づいて当該データと同等の印刷物を生成する場合だけでなく、前記対象データを表示装置に表示して閲覧する場合をも意味する。従って、この発明を閲覧に適用する場合には以下に用いる「印刷」を含む言葉（例えば「印刷データ」）は「閲覧」（「閲覧データ」）となる。また、ハードディスク等の不揮発性記憶媒体と、ワークメモリとを区別するため、ワークメモリの参照符号にはMを付している。

15

（第1の実施の形態）

第1図は本発明の第1の実施の形態を示すブロック図であり、第2図はパーソナルコンピュータの使用環境の構成図を示すブロック図であり、第3図は以下に説明する禁止情報の例を示す図であり、更に第4図は、第1図の部分を更に詳しく表したブロック図である。

20 第2図に示すように、パーソナルコンピュータ1（以下、PC1と記述する。）に種々のアプリケーション・ソフトウェアを搭載して簡易な印刷システムを構成した場合には、編集処理、画像処理（色処理）を行うことが可能となる。スキヤナ3を入力手段とした場合、該スキヤナによって取り込まれた画像データがP
25

C 1 に入力され、複製手段としてのプリンタ 2 は P C 1 の印刷データに従って用紙、O H P 用紙等に印字イメージの像形成を行うことになる。

P C 1 がネットワーク 1 0 0 に接続されている場合、ネットワーク 1 0 0 上のネットワークスキャナ 5 から画像を取り込んだり、ネットワークプリンタ 4 に印刷データを転送して印刷もできるようになっている。

D T P システムは、前記のように目的の原稿を P C 1 に取り込むスキャナ 3 と、当該スキャナから取り込んだ画像に色処理、加工処理を行う P C 1 と、当該画像を印刷するプリンタ 2 で構成され、前記スキャナより取り込まれる画像に変えて、P C 1 に搭載されたアプリケーションを使用して描かれた図形でもよいことはもちろんである。

次に、第 1 図を用いて、P C 1 が特定の印刷データ 1 1 を印刷する場合の動作を説明する。

第 1 図はパーソナルコンピュータ 1 が特定の印刷アプリケーションの下で動作する場合の機能ブロック図である。スキャナ等を介して外部から入力された画像データ、あるいは、C P 1 の内部で画像生成用のアプリケーションを用いて生成された画像データは、印刷データ 1 1 として印刷情報メモリ M 1 1 に収容されている。この状態でユーザより印刷指定が行われると、プリンタドライバ 1 2 に渡される。ここで、印刷情報メモリ M 1 1 はワークメモリを想定しており、このワークメモリにはハードディスク等に予め記憶された印刷データ 1 1 が渡される場合、あるいは、刷データ 1 1 がスキャナ等から直接渡される場合等が考えられる。

プリンタドライバ 1 2 は、P C 1 からプリンタ 2 にデータの橋渡しを行う制御プログラムとして、予めインストールされているものである。このプリンタドライバ 1 2 はアプリケーションより印刷指定された印刷データ 1 1 をプリンタ 2 に転送する。

25 第 1 図において、データ監視手段 4 0 0 は印刷情報解析回路 1 5 と複製禁止情

報 1 1 を収容する禁止情報メモリ M 1 4 とより構成されている。尚、禁止情報メモリ M 1 4 には、後述するハードディスク等の禁止情報記憶手段 3 0 0 より必要に応じて複製禁止情報が渡されるようになっている。尚、この複製禁止情報 1 4 は、文書、紙幣、証券、金券などあらゆる印刷物を対象に、印刷情報を特定できるものであれば何でもよい。また、その種類は 1 種類に限らず、後述するように種々の種類が考えられる。更に、前記印刷情報メモリ 1 1 と禁止情報メモリ 1 4 は上記印刷情報メモリ M 1 1 と同様ワークメモリである。

前記印刷データ 1 1 はプリンタドライバ 1 2 よりプリンタ 2 に渡されるとともに、データ監視手段 4 0 0 を構成する印刷情報解析回路 1 5 にも渡される。この印刷情報解析回路 1 5 はプリンタ 2 に転送される印刷データ 1 1 のページ記述言語などで記載された文字列情報、画像パターン情報、コード情報、電子透かし技術で埋め込まれた暗号情報などの複製要素を確認メモリ M 1 6 上に展開する。ここで展開とは必ずしもピットマップデータへの展開を意味するもではなく、プリンタが印刷可能な形式のデータを展開することを意味している。例えば、ディスプレイリストのような中間言語、文字であればアスキーコードの状態でもよい。尚、前記コード情報とはあるコード（番号、符号等）に対応する特定のパターンを意味し、後述するコード解析エンジンによって解析されることによって、前記番号、符号にデコードされる情報をいう。

更に、前記印刷情報解析回路 1 5 はこのようにして展開された印刷データ 1 1 の複製要素と、禁止情報メモリ M 1 4 に収容された複製禁止情報 1 4 との照合および解析を行なう（後に詳しく説明）。ここで、印刷データ 1 1 の前記複製要素が予め禁止情報メモリ M 1 4 に登録されている複製禁止情報 1 4 の 1 つと一致していると判定された場合は、プリンタドライバ 1 2 に対して印刷データの転送を停止させる停止命令 1 5 1 を出力する。この停止命令 1 5 1 によって、プリンタドライバ 1 2 に備えた禁止手段 1 2 1 は、印刷データのプリンタ 2 への転送を停止

する。

前記の方法によって不正な印刷を P C 1 を通過する段階で防止できることになる。

前記の複製禁止情報 1 4 の内容は、印刷を禁止をしようとする内容に対応して、
5 更新できるようになっている。これによって、日々変更される機密管理レベル、
機密情報、日進月歩で技術開発が進歩する偽造防止技術、暗号化技術に迅速に対
応できる。

すなわち、更新手段および取得手段としての情報更新回路 1 3 には、あらかじ
め更新権利者の I D を登録しておく一方で、 I C カード 2 0 0 にも更新権利者で
10 あることを意味する I D が記録されている。この状態で、該 I C カード 2 0 0 が
P C 1 のカード読み込み手段に挿入されると、前記情報更新回路 1 3 が I C カー
ド 2 0 0 の認証を行うようになっている。

ここで、正当な更新権利者による更新行為であると認証された場合にのみ、 I
C カード 2 0 0 に保存された更新データを取得し、ハードディスク等の禁止情報
15 記憶手段 3 0 0 に既に書き込まれている内容（もちろん新規に書き込むばあいも
ある）複製禁止情報 1 4 を更新する。

尚、 I C カード 2 0 0 自体の更新は複製禁止情報 1 4 のマスタとなる情報（マ
スタ禁止情報）を収容したサーバ装置（例えば第 1 1 図に示す複製禁止登録装置
6 ）とそれを駆動する別途の P C 等で実行することになる。この I C カード 2 0
20 0 の更新時にはその日付（あるは更新された内容のバージョン）を更新履歴とし
て I C カードに記憶しておく。一方で、禁止情報記憶手段 3 0 0 の内容が当該 I
C カードに基づいて更新されたときにもその日付（あるは更新された内容のバ
ージョン）を禁止情報記憶手段 3 0 0 に記憶しておき、 I C カードの日付（バージ
ョン）の方が新しい場合にのみ、情報更新回路 1 3 が禁止情報記憶手段 3 0 0 の
25 内容を更新するのが好ましい。これによって、不要な更新処理を避けることができ

る（第5の実施の形態参照）。

前記更新データはネットワーク100を経由して入手してもよい。すなわち、ネットワーク上に、複製禁止情報14の原情報となるマスタ禁止情報を収容したサーバ装置（例えば第11図に示す複製禁止情報登録装置6）を配設しておく。

5 ここで、前記情報更新回路13は、前記ネットワーク上の前記サーバ装置を定期的にあるいは必要に応じてアクセスして前記サーバ装置よりマスタ禁止情報を取得する（第5の実施の形態参照）。

尚、上記のようにネットワークを介して複製禁止情報を取得する場合も、禁止情報記憶手段300に収容された複製禁止情報が前回更新された日付等と、前記10サーバ装置上の原情報が更新された日付等に基づいて、最新の情報のみを禁止情報記憶手段300に取り込むようにするのが好ましい。

また、ネットワーク上のサーバ装置に更新権を持つ者のIDを登録しておき、ネットワークを介して送られる更新者の個人ID等に基づいて、当該更新指示者が正当権利者であるか否かの判断をする構成とすることも可能である。すなわち、15前記情報更新回路13は上記ICカードに登録された更新権の情報をそのユーザのIDとともに上記サーバ装置に転送すると、更新権のない者からの更新要求である場合はマスタ禁止情報（複製禁止情報）をPC側に転送しないようにする。但し、ここで使用するICカードには上記の場合と異なって、当該ICカード自身に複製禁止情報を書き込む必要はない。

20 このように、更新機能を持つことで、複製禁止情報の更新が簡単に行え、最新の状態に内容を維持することができる。また、機器に内蔵したメモリ（ROM）の交換が不要となるので、更新を迅速に行うことができるとともに、不正印刷の広がりの拡大を防止できる。

また、更新権利者の認証を行うことで、情報の改ざん、不正な印刷を行う者に対する防御をすることができる。

前記のようにして取得される複製禁止情報 1 4 は複製処理時に前記禁止情報記憶手段 3 0 0 から禁止情報メモリ M 1 4 に第 3 図に示すようにして収容される。

前記禁止情報メモリ M 1 4 のフィールド F 1 4 1 には、文書中のタイトル、文書中の特定文字列（例えば、機密文書の主要なキーワードなど）等の文字情報 1 4 1 が保存される。フィールド F 1 4 2 には、印刷情報を特定できる固有の画像パターン情報 1 4 2 が保存される。フィールド F 1 4 3 には、コードの解析情報（コード情報） 1 4 3 が保存される。例えば、特定のパターン（あるいは文字列）が特定のコードに対応するときには、当該パターン（あるいは文字列）とコードの対応関係の情報が保存される。

10 更に、フィールド F 1 4 4 には、著作権で保護された写真画像データに埋め込まれた電子透かし解読情報や、スキャナ 3 で読み込む原稿に予め所定の暗号化（セキュリティ印刷等）によって印刷されている暗号パターンの解読アルゴリズム、コードの種別情報などの暗号情報 1 4 4 が保存される。

15 この複製禁止情報 1 4 は、必要な情報を追加するだけで、あらゆる文書、原稿に対応できる。また、出力手段としてプリンタではなく表示装置を用いた場合にも適用できる。

20 例えば、C R T 等のディスプレイを用いた表示システムに本発明のデータ監視方法を適用する際には、前記各複製禁止情報に加えて閲覧（複製）禁止に係る静止画像あるいは動画像情報に埋め込まれた特定の図形、コード等を複製禁止情報として追加することで足りる。

次に、印刷情報解析回路 1 5 は第 4 図に示すように、プリンタドライバ 1 2 を常に監視し、印刷を開始する際に必ず所定の動作を行うようとする。

25 まず、印刷情報解析回路 1 5 が動作を開始すると、描画エンジン 1 5 4 は、プリンタドライバ 1 2 から印刷データ 1 1 を構成する複製要素を入手し、確認メモリ M 1 6 に当該複製要素に従って、各複製要素の描画処理を行う。このように、

確認メモリM16に描画された各複製要素161は、各種の解析エンジンによつて、内容が解析される。

すなわち、確認メモリM16に展開された対象データ（印刷データ11）の複製要素161のうち、タイトルデータがタイトル解析エンジン155によって抽出され、その内容の解析結果を照合回路159に転送する。照合回路159は禁止情報メモリM14に収容された複製禁止情報14の中から、照合情報として使える文字情報141を選び出し、前記のようにタイトル解析エンジン155が転送してきた解析結果と照合する。照合の結果、一致する情報が発見されると不正印刷の印字と見なし、停止命令151に基づいてプリンタドライバ12の印刷動作を停止させる。

尚、前記タイトル解析エンジン155がタイトルを抽出する手法は種々考えられるが、一般的には、対象データの内からサイズの大きな文字が集合している領域をタイトル領域として抽出してタイトルと見なす処理をしている。

同様に、文書解析エンジン156は、確認メモリM16に展開された複製要素からテキストデータを抽出して照合回路159に渡す。また、イメージ解析エンジン157は確認メモリM16に展開された複製要素から写真部分を抽出して照合回路159に渡す。更に、コード解析エンジン158は確認メモリM16に展開された複製要素をデコードして特定のコード（数値、記号）を抽出し、照合回路159に渡すようになっている。

前記照合回路159は複製禁止情報14の中から、照合情報として使える文字（テキスト）情報141、画像パターン情報142、コード情報143、暗号情報144をそれぞれ選択し、前記の各種解析エンジンから転送されてくる解析結果と照合する。前記照合の結果、いずれかの複製禁止情報と一致する印刷情報が検出されると不正印刷と見なし、停止命令151によってプリンタドライバ12の印刷動作を停止させる。

上記の照合手順において、照合回路 159 は、各解析エンジンからの問合わせに応じ、複製禁止情報 14 の中から必要な情報を入手して各解析エンジンに返答するようになっている。例えば、前記、コード解析エンジン 158 が暗号の解読をするときには、デコードアルゴリズムとその鍵を必要とするが、コード解析エンジン 158 は、暗号の解読に必要なデコードアルゴリズムを照合回路 159 に問い合わせて最新の解読アルゴリズムを、上記禁止メモリ M14 から入手して、暗号を解読をする。また、特定のコードを正規の情報に変換するときも、当該コードと対応する正規情報との対応関係が必要であるが、この場合も照合回路 159 が当該対応関係を上記禁止メモリ M14 から入手してコード解析エンジン 158 に渡すようになっている。

このように、複数の解析エンジンを有することで、文書特徴の異なる様々な印刷原稿に対応できる。

本願発明のデータ監視装置に、機密管理機能を与えると更にその効果を有効にすることができる。

15 ネットワークを介しての機密管理機能は第 7 の実施の形態の記載に譲るとして、ここではデータ監視装置のみで実行される機密管理機能について説明する。

すなわち、各複製禁止情報に機密管理のレベルを示す機密管理情報 67 を例えば第 13 図に示すように与えておく（第 13 図に内容については第 7 の実施の形態で説明する）。他方で、P C 1 のユーザに当該ユーザ ID とともに機密管理レベルを与えておき、この内容を例えば I C カード 500 に登録しておく。この状態で、ユーザが当該 P C 1 を使用する前に、I C カード 500 を機密管理回路 68 に読ませると、当該機密管理回路 68 はその内容を、防止解除設定手段 17 に渡す。防止解除設定手段 17 は、上記のように印刷データ 11 の複製要素が確認メモリ M16 に展開されたとき、印刷情報解析回路 15 で解析処理をしている複製要素の機密管理情報 67 を参照して、現在のユーザが当該複製要素を複製、閲覧

できる権限を持っているか否かを判断する。これによって、複製、閲覧の権限のある者がユーザであるときには、印刷除法解析回路 15 の禁止処理を解除することになる。

これによって、複製、閲覧の禁止をする必要のない場合にまで、印刷除法解析 5 回路 15 が作動することを防止できるようになっている。

尚、上記 I C カード 500 は、上記更新権を登録した I C カードと共にしてもよいが、上記更新権と機密管理レベルは別のデータとして扱うのが好ましい。

上記の機密管理処理は、以下に説明するプリンタ、スキャナにも適用できることはもちろんである。

10 以上、第 1 の実施の形態によれば、P C 1 からプリンタに印刷を行う際に印刷内容を解析し、不正印刷を防止する機能を持たせることで、社内の機密文書の不正印刷、紙幣、金券の偽造などを未然に防ぐことができる。さらに、不正印刷情報を簡単に更新できる仕組みを持つことで、日々変更される機密管理レベル、機密情報、日新月歩で技術開発が進歩する偽造防止技術、暗号化技術に迅速に対応 15 できる。結果、不正印刷の広がりの拡大を防止できる。

また、更新権利者の認証確認を行うことで、情報の改ざん、不正な印刷を行う者に対する改造防止ができる。また、管理レベルを持たせることもでき、機密情報の管理を様々な階層レベルで実現できる。

20 また、パーソナルコンピュータに不正印刷防機能を持たせる場合は、特別なハードウェアは不要で、ソフトウェアのみをインストールすれば良く、低成本で実現できる。

(第 2 の実施の形態)

第 1 の実施の形態ではパーソナルコンピュータに不正印刷防止機能を組み込む場合を説明したが、ここではプリンタに不正印刷防止機能を持たせる実施の形態 25 を説明する。

まず、第2図、第5図を用いて、プリンタ2の動作を説明する。第5図はプリンタ2のブロック図である。

プリンタ2はPC1からの印刷データを受信バッファ21で受け、コマンド解析回路22に順次印刷データを転送する。コマンド解析回路22は受け取った印刷データの言語、画像データフォーマットを解析する。次に、コマンド解析回路22が解析処理をした結果、文字、図形描画を行う必要があれば、図形／文字描画回路23に印刷データを転送する。図形／文字描画回路23は、メモリコントローラ25を経由して、画像メモリM26に所定の描画動作を行う。同様に、コマンド解析回路22が解析処理をした結果、写真データを展開する必要があれば、10 イメージ描画回路27に印刷データを転送する。イメージ描画回路27は、メモリコントローラ25を経由して、画像メモリM26に所定の写真データを展開する。メモリコントローラ25は画像メモリM26に所望の画像データが形成されるとプリンタエンジン24に当該画像データを転送し、該プリンタエンジン24は、受け取った画像データに基づいて紙に印刷を行うようになっている。

15 第5図において、データ監視手段400は、印刷情報解析回路28と複製禁止情報29を収容する禁止情報メモリM29により構成される。

前記データ監視手段400を構成する前記印刷情報解析回路28は、前記のように画像メモリM26に展開される画像データを監視し、プリンタエンジン24に画像データが転送される前に、画像データの内容を解析する。もし、画像データの内容が、複製禁止情報29に保存された情報と一致した場合は、停止命令218が出力され、当該停止命令218を受けてプリンタエンジン24に備えた禁止手段241が当該プリンタエンジン24の動作を停止する。

次に、更新手段としての更新回路30の機能は前記第1の実施の形態で説明した内容とほぼ同一であるのでここで異なる点を中心に説明する。尚、第1の実施25 の形態における禁止情報メモリM14、情報更新回路13が第2の実施の形態の

禁止情報メモリ M 2 9、情報更新回路 3 0 に対応する。また、禁止情報記憶手段 3 0 0 としてはハードディスクでもよいが、プリンタでは記憶すべきデータが大量にある訳ではないので、フラッシュメモリ等の小容量の書き換え可能な不揮発性メモリを使用するのが好ましい。

5 I C カード 2 0 0 による更新の手順は第 1 の実施の形態と同じである。また、更新データは P C 1 より入手してもよい。P C 1 は印刷データの他に、定期的、不定期、印刷時のいずれでもよいが、更新データをプリンタ 2 に転送する。この更新データは、受信バッファ 2 1 経由して前記コマンド解析回路 2 2 が受ける。このときコマンド解析回路 2 2 は印刷データと別に定義された命令コードから更新データ 2 2 1 を検出し、当該更新データ 2 2 1 を更新回路 3 0 に転送する。

10 前記 P C 1 より得られる更新データは、ネットワーク 1 0 0 を介して P C 1 が取得するものであっても、可搬記憶媒体から P C 1 が取得するものであってもよい。この場合更新権の確認は P C 1 側でなされていることになる。

15 尚、この実施の形態に使用する複製禁止情報 2 9 の内容は前記第 1 の実施の形態で説明した複製禁止情報 1 4 と全く同じであるので説明を省略する。

次に、第 6 図に示した、印刷情報解析回路 2 8 は第 4 図に示した印刷情報解析回路 1 5 と略同じである。第 1 の実施の形態におけるように P C 1 内での処理はプリンタドライバ 1 2 よりの印刷データを描画エンジン 1 5 4 で確認メモリ M 1 6 に展開する必要があるが、本実施の形態の場合は、画像メモリ M 2 6 に P C 1 より転送される印刷データが展開される。

20 このように印刷データが展開されて以降の処理あるいは、回路は参照符号が異なるのみで、前記第 1 の実施の形態と同じである。

25 以上の構成による効果も前記 P C に対して本発明を適用した場合と同じであるが、ここでは動画に対する複製禁止はできない。ただ、動画の各フレームをプリンタで出力しようとした場合は前記各エンジンを稼働させることは可能である。

(第3の実施の形態)

第2の実施の形態ではプリンタに不正な複製を防止するデータ監視機能を組み込む場合を説明したが、ここではスキャナにデータ監視機能を持たせる実施形態を説明する。

5 第7図を用いて、ネットワークスキャナ5の動作を説明する。第7図はネットワークスキャナ5のブロック図である。

対象となる原稿（図示せず）をイメージセンサ51によって読み取り、A/D変換器52によってデジタル画像データに変換する。ここで、画像中の文字等のエッジを強調するエッジ強調処理、カラー処理等画像処理が画像処理回路53で行われ、ネットワークインターフェース54（以下、ネットワークI/F54と記す。）を経由して、画像データのネットワークへの転送が行われる。

データ監視手段400は入力情報解析回路55と複製禁止情報56を収容する禁止情報メモリM56より構成される。このデータ監視手段400を構成する入力情報解析回路55は複製禁止情報56に保存された情報に基づいて印刷が禁止されている原稿かどうかの判定を行う。ここで、禁止されている原稿を検出した場合は、停止命令551をネットワークI/F54に出力し、当該停止命令551を受けてネットワークI/F54に備えた禁止手段541が画像データの出力を停止する。

禁止情報メモリM56に収容された複製禁止情報56は第3図に示す複製禁止情報14と同様であるのでここでは説明を省略する。また、前記複製禁止情報56は前記第1の実施の形態あるいは第2の実施の形態と同様の手順で、情報更新回路57によって、更新可能である。該情報更新回路57による更新手順も前記第1の実施の形態、あるいは第2の実施の形態で説明したように、ネットワーク上に接続された他の機器からネットワークI/F54を経由して取得してもよいし、あるいは、着脱可能なICカード200、あるいはメモリカードからの更新

情報から取得してもよい。尚、前記第2の実施の形態と同様に、禁止情報記憶手段300としてはハードディスクでもよいが、ネットワークスキャナでは記憶すべきデータが大量にある訳ではないので、フラッシュメモリ等の不揮発性メモリを使用するのが好ましい。

5 この実施の形態では上記のように、ハードディスクやフラッシュメモリを用いないで、ネットワーク上にあるサーバ（マスタ情報記憶手段）から、直接複製禁止情報を取得する場合を考察する。

スキャナ5には登録情報要求回路58（情報取得手段）を設ける一方、ネットワーク上には第5の実施の形態で説明するように、前記複製禁止情報56の原情報（複製禁止情報56と内容は同じ）を収容したサーバ装置（例えば第10図に示す複製禁止登録装置6）を配設しておく。そして、前記登録情報要求回路58によりネットワークを経由して複製禁止情報56を入手することができる。これによって、膨大な情報を格納するメモリを搭載する必要がなく、製品コストを削減できる。

15 ここで、前記ネットワーク上のサーバ装置が、特定の事業所のいずれか場所に設置されたサーバである場合を想定する。この場合、入力情報解析回路55が原稿の読み取時に自動的に登録情報要求回路58を起動して前記サーバ装置にアクセスし、必要な複製禁止情報56を入手する仕組みを持つようとする。この複製禁止情報56は当該ネットワークスキャナ5の中ではハードディスク等に収容しないで、直接ワークメモリである禁止情報メモリM56に収容され、入力情報解析回路55での比較照合に供される。

この登録情報要求回路58の適用は、前記第1の実施の形態でのパソコンコンピュータあるいは、第2の実施の形態でのプリンタにも適用できることはもちろんである。

25 なお、本実施の形態のスキャナとしては、ネットワークを介してPC1に接続

される場合だけでなく、P C 1 に直接接続されるスキャナにも適用できることはもちろんである。

以上、第 3 の実施の形態によれば、ネットワークスキャナ 5 は、複製禁止情報 5 6 と同様の内容を登録情報要求回路 5 8 によってネットワークを経由して入手するので、膨大な情報を格納するメモリを搭載する必要がない。従って、プリンタやスキャナ等、通常はハードディスクを持たない機器に適用すると有益である。

禁止情報記憶手段 3 0 0 を備えて I C メモリ 2 0 0 あるいはネットワークを介して、当該禁止情報記憶手段 3 0 0 の内容を更新する場合の効果は、上記第 1 、第 2 の実施の形態と同じであるので説明を省略する。

10 (第 4 の実施の形態)

第 3 の実施の形態ではスキャナにデータ監視機能を組み込む場合を説明したが、ここではネットワークプリンタにデータ監視機能を持たせる実施の形態を説明する。

第 8 図はネットワークプリンタ 4 のブロック図である。

15 ネットワークプリンタ 4 はネットワーク上に接続された機器から印刷データを受け取る。コマンド解析回路 4 2 はネットワークインターフェース 4 1 (以下、ネットワーク I / F 4 1 と記す。) を経由して印刷データ、命令コマンドのやりとりを行うとともに、受け取った印刷データの言語、画像データフォーマットを解析する。更に、前記コマンド解析回路 4 2 、図形／文字描画回路 4 3 、イメージ描画回路 4 7 、メモリコントローラ 4 5 は前記第 2 の実施の形態説明したプリンタにおける場合と参照符号が異なるのみで、機能は同じであるのでここでは説明を省略する。

前記メモリコントローラ 4 5 は画像メモリ 4 6 に所望の画像データが形成されるとプリンタエンジン 4 4 に画像データを転送する。プリンタエンジン 4 4 は、25 受け取った画像データから紙に印刷を行う。

データ監視手段 400（刷情報解析回路 48 + 禁止メモリ M49）を構成する
印刷情報解析回路 48 は、コマンド解析回路 42 で解釈される印刷データを監視
し、プリンタエンジン 44 に画像メモリ 46 から印刷データが転送される前に、
画像データの内容を解析する。もし、画像データの内容が、禁止情報メモリ M4
5 9 に収容された複製禁止情報 49 のいずれかと一致した場合は、停止命令 481
を出力し、当該停止命令 481 を受けた、プリンタエンジン 44 に備えた禁止手
段 441 がプリンタエンジン 44 の動作を停止する。第 2 の実施の形態と同様に、
印刷情報解析回路 48 は画像メモリ 46 を監視し解析してもよい。
次に、更新回路 31 は、前記の各実施の形態での更新回路 30、31、57 と
10 同様、禁止情報記憶手段 300 に収容された複製禁止情報 49 の内容を、禁止し
たい内容に合わせて更新できる。この複製禁止情報 49 の更新方法の種類、およ
び更新手順は前記各実施の形態で説明した内容と同じであるので、説明を省略す
る。尚、ネットワークプリンタは本来ネットワークに接続されたプリンタである
ので、上記第 3 の実施の形態と同様、ネットワーク 100 を介して複製禁止情報
15 の更新を行うのが有益である。

（第 5 の実施の形態）

第 1 から第 4 の実施の形態ではデータ監視機能を組み込んだ装置について説明
したが、ここではデータ監視機能を組み込んだ装置に対して、複製禁止情報を迅
速に配信できる方法の一実施例を説明する。すなわち、上記各実施の形態で説明
20 した P C、スキャナ、プリンタはサーバ装置（複製禁止登録装置）に集約した複
製禁止情報の配信を受けるようにすると、装置間で複製禁止情報を共通にするこ
とができる。

第 9 図、第 10 図を用いて、印刷を禁止したい情報の登録機能について説明す
る。第 9 図はネットワーク上に接続された機器への登録機能を説明する図であり、
25 第 10 図は複製禁止登録装置のブロック図である。

不正な複製を防止するためには、いかに迅速に目的とする複製物を検出し、複製を防止するかが重要である。第9図に図示する複製禁止登録装置6はネットワーク100上に接続されたネットワークスキャナ5、ネットワークプリンタ4、パーソナルコンピュータ1、第nのネットワークプリンタ7に対して、複製禁止情報5をネットワーク経由で配信する装置である。

各装置に組み込まれた不正印刷防止機能は、個々に組み込まれた更新手段（更新回路13、30、31、57）によって、複製禁止登録装置6からの更新データを取得し、複製禁止情報の内容を最新のものに更新する。これによって、ユーザーに負担をかけることなく、迅速に不正印刷の情報を各機器に伝達でき、不正な複製を未然に防止できる。

次に、第10図を用いて、複製禁止登録装置6の詳細を説明する。第10図は複製禁止情報登録装置のブロック図である。

第10図において、情報設定手段66は、例えばフロッピーディスク、CD-R OM等の記録媒体150より複製禁止情報の原情報であるマスタ禁止情報65を取得する。

また、前記マスタ禁止情報65の入力方法としては、上記可搬性の記憶媒体を用いる場合の他、キーボードから情報設定手段66に直接入力する方法、スキャナなどから画像パターンを入力する方法が考えられる。このようにマスタ禁止情報を取得した情報設定手段66は、当該マスタ禁止情報65をマスタ情報記憶手段800に書き込むことになる。もちろん既にマスタ禁止情報65が書き込まれている場合はその内容は更新されることになる。

マスタ禁止情報65を更新する別な方法としてネットワーク100を経由する方法もある。この場合は、登録情報自動更新手段64に、予め決められたデータベースを指定して更新データ入手するように設定しておく。更新記録があったときは、更新履歴情報63（例えば更新日時、あるいは更新内容のバージョン）

を履歴記憶手段 801 に保存しておく。これによって、更新処理時にネットワーク上のデータベースの更新日と自機の更新日を比較することによって、登録情報自動更新手段 64 が複製禁止情報 65 を更新する必要が「ある」か、「ない」かを判定できる。この、更新周期は所定の時間間隔でもよいし、予め決められたデータベースからの通知に従ってもよい。前記マスタ情報記憶手段 800 と履歴記憶手段 801 は同じハードディスクの異なる領域を使用することで足りる。

情報開示／配信手段 62 は、ネットワーク 100 を経由した要求（第 3 の実施の形態参照）に対し、マスタ情報記憶手段 800 に収納されたマスタ禁止情報 65 を複製禁止登録情報として転送する。また、当該複製禁止登録装置 6 の管理下に置かれた機器、例えばプリンタ、スキャナ、パーソナルコンピュータの更新回路 13、31、57 からの更新要請に対してマスタ禁止情報 65 を複製禁止登録情報として配信する。

尚、前記禁止情報記憶手段 800 と履歴記憶手段 801 は同じハードディスクの異なる領域を使用することで足りる。

前記複製禁止登録装置 6 の管理下に置かれた機器として、第 4 の実施の形態で説明したネットワークプリンタ 4 を用いた場合を説明する。ネットワークプリンタ 4 では、更新回路 31 よりネットワークを介して更新要請があったとき、情報開示／配信手段 62 が作動して、禁止情報記憶手段 800 に収容された複製禁止情報 65 を配信する。このとき、履歴記憶手段 801 から現在禁止情報記憶手段 800 に書き込まれている複製禁止情報 65 の更新履歴も同時に配信される。

これを受けて、前記更新回路 31 は既に禁止情報記憶手段 300 に収容されている複製禁止情報 49 に変えて当該複製禁止情報情報 65 を書き込むことになる。このとき、更新回路 31 は前回の更新処理で履歴記憶手段 301 に記憶された更新履歴情報 32 と、前記更新履歴情報 63 を比較して更新の必要があるか否かを判断することになる。これによって、当該ネットワークプリンタ 4 が起動（電源

ON) したとき等、必要に応じて、禁止情報メモリ M 4 9 に前記複製禁止情報 4 5 がダウンロードされることになる。尚、禁止情報記憶手段 3 0 0 と履歴記憶手段 3 0 1 は同じハードディスクの異なる領域を使用することで足りる。

また、ネットワークプリンタ 4 には先に第 3 の実施の形態（スキャナ）の場合 5 で説明したと同様の登録情報要求回路 3 3 （情報取得手段）が備えられることも可能である。このように、登録情報要求回路 3 3 を備えたとき、例えば画像メモリ 4 6 に印刷データが展開された段階で、印刷情報解析回路 4 8 の指示に基づいて、登録情報要求回路 3 3 が必要な複製禁止情報の要求を実行し、情報開示／配信手段 6 2 から直接に禁止情報記憶手段 8 0 0 に収容された複製禁止情報 6 5 を 10 取得し、禁止情報メモリ M 4 9 に収容することもできる。

これによって、ネットワークプリンタ側は複製禁止情報 4 9 の保存メモリが不要になり、コストを削減できる。また、禁止印刷登録情報 6 5 を更新すれば、ネットワークプリンタ 4 の複製禁止情報 4 9 も更新されることになるので、管理がしやすく、迅速な対応が可能となることになる。

15 前記のように更新回路 3 1 の実行した更新記録を、更新履歴情報 3 2 として禁止情報記憶手段 3 0 1 に保存すると、登録情報要求回路 3 3 が無効な要求をすることを防止できる。

以上、第 5 の実施の形態によれば、複製禁止情報登録装置 6 からネットワーク 20 に接続された各機器に対し禁止印刷登録情報 6 5 を開示／配信できるので、機器管理、機器メンテナンス、機密情報レベルの変更が行いやすい。

また、一ヵ所の情報変更で、ネットワーク上の管理された機器を一斉に更新することができるので、迅速に不正な複製を防止できる。

以上、ネットワークを介しての配信のみについて説明したが、上記のように一か所に集約された複製禁止情報を I C カード（例えば第 1 の実施の形態の I C カード 2 0 0）等に可搬記憶媒体を介して各装置に配信することでも、当該複製禁

止情報登録装置 6 は十分に機能する。

(第 6 の実施の形態)

第 11 図は、データ監視機能を組み込んだ装置に対して、不正複製防止機能を解除する方法の実施形態を示すブロック図である。

5 装置のメンテナンス等、何らかの都合により、不正印刷の防止機能を解除したい場合がある。機能を解除する権限を有するユーザは解除命令を行うことができる I C カード 201 を防止解除設定回路 17 に挿入する。防止解除設定回路 17 は、I C カード 201 の認証を行い、印刷情報解析回路 15 (28, 55) に機能停止を指示する。これによって、不正な複製を防止する機能を停止できる。

10 また、ネットワークから特定のパスワードが入力されたときやあるいはキーボードより特定の暗号解読の鍵が入力されたときに、印刷情報解析回路 15 (28, 55) の機能を停止するようにしてもよい。

15 いずれにしても、解除権限をもつユーザが特定できる方法であればよい。もちろん、防止解除設定回路 17 には、I C カード 201 の番号等認証に必要なデータをキーボードあるいはネットワークから登録できる機能を備えるようになっており、これによって、前記 I C カード 201 の認証が可能となる。これにより、組織の変更、機器の移動、機密レベルの変更等、様々な管理状態に迅速に対応できる。

20 以上、第 6 の実施の形態によれば、防止解除設定回路 17 を利用することで、機器メンテナンスができる。また、防止解除設定回路 17 は I C カードの番号等の登録機能をもつので、自在な管理を可能にする。

以上、第 1 ~ 第 6 の実施の形態によれば、迅速に不正な複製を防止することができる。

(第 7 の実施の形態)

25 データ監視機能をもつプリンタ 4 において、ネットワークを介して機密管理を

行う方法の一実施例を第12図、第13図を用いて説明する。第12図は機密情報管理の説明図であり、第13図は管理情報の内容の説明図である。

第12図において、マスタ禁止情報65の他に、機密管理情報67を複製禁止情報登録装置6のマスタ情報記憶手段800に持つことによって、機密情報の管理に対して、管理する情報の更新、アクセスする人に対する表示・印刷を許可する範囲の更新、などに迅速に対応できるようになる。

この機密管理を行う方法について説明する。上記第6の実施の形態で説明したように、マスタ禁止情報65は可搬記憶媒体あるいはネットワークを介してマスタ情報記憶手段800に収納されている。

この状態で、特定の管理者は、まず自分が更新権限を有することを通知するために複製禁止情報登録装置6にICカード700を挿入する。複製禁止情報登録装置6の情報設定手段66は、ICカード700の内容を読み取り、更新権限者か、そうでない人物かを確認する。更新権限者であれば、キーボード600とモニタ661を用いての機密管理情報67の入力を受け付ける。

上記情報設定手段66は、上記のようにして入力された機密管理情報67をマスタ禁止情報65と対にして、例えば第13図に示すテーブル670に書き込むようになっている。すなわち、テーブル670において情報IDはマスタ禁止情報（複製禁止情報）を特定するID、許可レベルは、例えばA, B, Cの順に、また更にA, B, Cの後に付された数字の大きい順に機密度が高くなる符号をいう、また、所属IDは前記マスタ禁止情報の管轄部署を意味し、個人IDはユーザを識別するIDをいう。これによって、たとえば、マスタ禁止情報（複製禁止情報）D001に対しては、A001以上の許可レベルを有する人で、かつX00に所属する人なら情報出力が許可される。さらに、個人でID1/PW1の人を対象として複製・閲覧を許可すると定義する。

このようにして入力された機密管理情報67はプリンタ4側では、機密管理回

路 6 8 によって参照される。すなわち、ユーザはプリンタ 4 を使用する前に I C カード 5 0 0 を機密管理回路 6 8 に挿入する。機密管理回路 6 8 は、 I C カード 5 0 0 の内容を読み取り当該 I C カードに登録された機密管理レベルすなわち、許可レベル、所属 I D、個人 I D をユーザ I D とともに読み取って保持する。

5 次いで、特定の印刷データを P C 等より受け取って画像メモリ M 4 6 (第 8 図 参照) に展開した段階で、登録情報要求回路 3 3 は実施の形態 5 で説明したよう に、ネットワークインターフェース 4 1 を経由し、複製禁止情報 6 5 を取得して禁 止情報メモリ 4 9 に収容するとともに、対応する機密管理情報 6 7 もテーブル 6 7 0 より取得して防止解除設定手段 1 7 に渡す。この防止解除設定手段 1 7 では 10 現在印刷情報解析回路 4 8 で照合の対象となっている複製要素に対応する機密管 理情報 6 7 と、前記のように機密管理回路 6 8 に保持されたユーザの機密管理レ ベルとを比較して、ユーザの機密管理レベルが機密管理情報 6 7 より高いときは、ユーザが許可対象者であるとして信号 4 8 1 により、プリンタエンジン 4 4 に対し印刷を許可し、この結果、所望の印刷物を得ることができる。

15 不許可対象者であれば、防止解除設定手段 1 7 に解除指定は行わず、特定の情 報に対し印刷を禁止するように設定を行う。印刷情報解析回路 4 8 は、複製禁止 情報 4 9 により、禁止対象が特定される信号 4 8 1 を用いてプリンタエンジン 4 4 を停止させる。

以上のように、機密情報の管理情報を登録する機能を持つことで、日々の更新 20 を迅速に行うことができる。また、プリンタ 4 に機密管理機能を持たせることで、 機密情報の登録装置との連携で、きめ細かい複製・閲覧制御を実現できる。許可 レベルによる役職階層での複製・閲覧許可のレベル制御、所属 I D による拠点、 組織単位による複製・閲覧許可の制御、個人 I D による特定者レベルでの複製・ 閲覧許可の制御など、非常にきめ細かく情報開示操作を実現できる。登録装置を 25 ネットワーク上に置けば、組織変更、レイアウト変更しても、迅速に機密情報の

管理を実現することができる。さらに、出力を禁止するデバイス情報、管理期間情報など、管理を必要とする事項について拡張できるようにしておけば、さらに良い。

なお、I C カード 5 0 0 による個人認証の他に、手の指紋などによる個人認証、5 顔の認識による個人認証、人の目の網膜の認識による個人認証でも良い。個人を特定できる方法であれば、いずれも利用できる。

また、プリンタを例に説明したが、表示装置に本発明のデータ監視機能を持たせ、機密情報管理応機能を個々の装置に付加することで、機密事項の不本意な開示を防止できる。

10 更に、特定のパーソナルコンピュータの表示装置に限らず、P D A (Personal Digital Assistant)、携帯電話、ノート P C などあらゆる携帯情報端末の表示装置にも、もちろん応用できる。

また、音声の出力装置（スピーカー）にも応用できる。図示しないが、機密管理情報 6 7 として、禁止するデバイス情報を付加すれば、画像情報の表示は許可するが、音声情報の出力は禁止するなど出力メディアに対する禁止制御も可能となる。

いずれにしても、機器毎に機密情報の管理機能を持たせることで、ネットワークに接続される、あらゆる機器・端末の開示レベルを制御することができる。

前記第 1 ～第 6 の実施の形態では、複製禁止情報を用いて複製を禁止する場合について説明したが、以下第 8 ～第 1 0 の実施の形態ではパーソナルコンピュータ、プリンタ、スキャナ等で不正複製物を出力した場合に、当該機器を特定し、迅速に追跡することができる構成を備えた実施の形態を説明する。

（第 8 の実施の形態）

25 第 1 4 図は、機器固有の識別情報をプリンタで印刷される印刷データに付加する情報付加回路のブロック図である。

情報付加回路 18 は、PC 1 に搭載される中央制御装置（以下、CPU と記述する。）に内蔵される CPU 識別情報 18 a を抽出し、その情報をプリンタドライバ 19 に送る。プリンタドライバ 19 は、印刷メモリ M 11 に収容された印刷データ 11 に CPU 識別情報 18 a を付加し、新たな印刷データとしてプリンタ 2 に出力する。ここで CPU は、PC 1 に固有かつ唯一なものであるので、ユーザを管理する情報として有効な情報原である。

同様に、情報付加回路 18 は、PC 1 に搭載されるアプリケーション登録情報 18 b を各アプリケーションソフト 92 から取得し、その情報をプリンタドライバ 19 に送る。登録情報としては、ユーザ登録情報、メールアドレスなど装置を使用しているユーザ情報や、日付情報などである。プリンタドライバ 19 は、印刷データ 11 にアプリケーション登録情報 18 b を付加し、新たな印刷データとしてプリンタ 2 に出力する。

アプリケーション登録情報 18 b は、インストール時のユーザ情報、ユーザーに配布される所定の製造番号、ユーザパスワードなどである。また、アプリケーションにユーザが設定するメールアドレスは使用ユーザの所在を突き止める情報として有効であり、複製物に関与したユーザ、場所、日時を特定する情報として有効な情報原となる。また、PC 1 のオペレーティングシステム（以下、OS と記述する。）の登録情報を用いても良く、搭載されるソフトウェアでユーザ特定、ソフトウェア特定ができるものなら何でもよい。

また同様に、情報付加回路 18 は、PC 1 に搭載されるハードウェア情報 18 c を抽出し、その情報をプリンタドライバ 19 に送る。プリンタドライバ 19 は、印刷データ 11 にハードウェア情報 18 c を付加し、新たな印刷データとしてプリンタ 2 に出力する。ハードウェア情報として、PC 1 の CPU が搭載される基板情報、ネットワークインターフェース 93 に設定されている IP アドレスを取得する。また、接続されるプリンタ 2 の情報をドライバより取得してもよい。

以上、第7の実施の形態によれば、機器若しくはソフトウェアの使用ユーザ、場所、日付を特定する情報を自動で検出し印刷データに付与することで、複製物の出所場所、日時、使用ユーザを追跡することができる。これによって、不正な複製物を出力した機器を迅速に突き止め、その印刷データの作成状況が証拠として残されるので、不正な複製物の拡散を抑え、機密情報の漏洩範囲を最小限にくい止める事ができる。

(第9の実施の形態)

第15図はプリンタに追跡機能を持たせた場合のブロック図である。

10 プリンタ2はPC1からの印刷データを受信バッファ21で受け、コマンド解析回路22に順次印刷データを送る。コマンド解析回路22は受け取った印刷データの言語、画像データフォーマットを解析する。

15 コマンド解析回路22は受け取った印刷データの言語、画像データフォーマットを解析すると共に、印刷データに自動的に付与される識別情報222（装置情報、ソフトウェア情報、ハードウェア情報等）を抽出し、特定情報付加回路80に渡す。

次に、第1の実施の形態で説明したように、前記のようにコマンド解析回路22が解析した結果に基づいて、図形／文字描画回路23が画像メモリM26に文字、図形の描画を実行し、また、イメージ描画回路27が画像メモリM26に写真データを写真データを展開する。

20 更に、前記特定情報付加回路80は、メモリコントローラ25を経由して、画像メモリM26に識別情報222を所定のパターンで変調して、前記画像メモリM26で展開される画像に付与する。例えば、第16図に示すように印刷データ261上に特定情報コード1000が付与される。また、直接にプリンタエンジン24に所定のパターンを送付して紙に印刷してもよい。

25 メモリコントローラ25は画像メモリM26に所望の画像データが形成される

とプリンタエンジン 2 4 に画像データを転送し、プリンタエンジン 2 4 は、受け取った画像データから紙に印刷を行う。

以上、第 8 の実施の形態によれば、プリンタ 2 が受け取った印刷データから付与されている特定情報を抽出し、プリンタ 2 の内部で印刷を行う際に、印刷データ上に、更にその特定情報を自動的に付与するので、社内の機密文書の不正複製、
5 紙幣、金権の偽造などが行われた場合に機器の追跡を行うことができる。

(第 10 の実施の形態)

第 17 図はネットワークに接続されたプリンタに追跡機能を持たせる場合のブロック図である。

10 プリンタ 4 は P C 1 等からの印刷データをネットワークインターフェース 4 1 を経由して受け、コマンド解析回路 4 2 に順次印刷データを転送し、前記コマンド解析回路 4 2 は受け取った印刷データの言語、画像データフォーマットを解析する。

15 次に、図形／文字描画回路 4 3 による文字、図形の描画処理、イメージ描画回路 4 7 による写真データを展開処理は前記第 1 の実施の形態あるいは第 8 の実施の形態と同じであるので説明を省略する。

特定情報付加回路 8 0 は、ネットワークインターフェース 4 1 からプリンタ 4 に付与されている I P アドレス 2 2 3 抽出し、メモリコントローラ 4 5 を経由して、画像メモリ 4 6 に I P アドレス 2 2 3 を所定のパターンで変調して展開画像 20 に付与する。付与する形態は、例えば第 8 の実施の形態同様に、第 16 図に図示するように印刷データ上に特定情報コード付与される。この I P アドレスは上記第 9 の実施の形態に示すようにコマンド解析回路 4 2 から抽出してもよいことはもちろんである。また、直接にプリンタエンジン 4 4 に所定のパターンを送付して紙に印刷してもよい。

25 メモリコントローラ 4 5 は画像メモリ 4 6 に所望の画像データが形成されると

プリントエンジン44に画像データを転送する。プリントエンジン44は、受け取った画像データから紙に印刷を行う。

以上、第9の実施の形態によれば、ネットワークに接続されたプリンタ4の識別情報(ＩＰアドレス)がプリンタ4の内部で印刷を行う際に、印刷データ上に、
5 更に自動付与されるので、社内の機密文書の不正複製、紙幣、金権の偽造などが行われた場合に、この機器、どの場所で印刷されたかを簡単に特定でき、追跡を行うことができる。これにより、機密情報の拡散を防止できる。

なお、本発明の複製装置は、CPU、DSPによるソフトウェアによって実現できる。また、専用のハードウェアによって実現してもよい。
10 また、機密文書管理ソフトウェアとしてデータベース、流通システム、電子メール等の文書交換ソフトウェア、ドキュメントの配信ソフトウェアに組み込むことも、もちろんできる。

また、静止画像にとどまらず、動画画像にも同様に適用でき、動画データ管理にも応用することができる。
15 さらには、スキャナ、プリンタ、パーソナルコンピュータ上で、原稿画像データ、文書テキストデータ、暗号データなど様々な特徴のデータに対応できることから、印刷に限らず、モニター表示にも利用できる。

以上のように、本発明によれば、複製禁止情報を更新可能としたので、原稿、電子データ等の不正な複製・閲覧を未然に、かつ迅速に防止することができる。
20 更に、機密管理機能を備えるようにしたので、特定のユーザに与えられた機密管理レベルとの関連で、複製・閲覧が許可されるユーザに対しては上記の禁止をかけないようにする効果がある。

更に、印刷データに該印刷データが処理された機器の識別が可能な情報を追加することによって、不正に複製された複製物の出所を追跡することが可能となる。
25 尚、上記の各実施の形態における各手段はハード構成でも実現可能であるが、

CPUと該CPUに搭載されるプログラムとを用いても実現可能である。

産業上の利用可能性

上記したように本発明は、事業所の文書、図面等の不正複製・閲覧の防止に適用できる。また、同一事業所であっても、特定の情報を複製・閲覧が許可されたユーザと許可されていないユーザの区別ができる。更に、より一般的に紙幣、金券等の複製の禁止、複製物を生成した装置の追跡に適用できる。

請求の範囲

1. 禁止情報記憶手段に収容されるとともに更新可能な少なくとも 1 種の複製禁止情報に基づいて、少なくとも 1 種の複製要素より構成される監視対象データの各複製要素を監視する監視処理と、前記監視処理によって、前記各複製要素が前記複製禁止情報の 1 種と一致すると見なされたときに監視対象データの入力または出力を禁止する禁止処理とを備えたことを特徴とするデータ監視方法。
5
2. 更に、前記更新処理時に更新権限を持つ者の更新処理である場合にのみ更新をする請求項 1 に記載のデータ監視方法。
- 10 3. 前記複製禁止情報の更新情報は、可搬記憶メディアによって提供される請求項 1 に記載のデータ監視方法。
4. 前記複製禁止情報の更新情報は、情報提供媒体によって提供されることを特徴とする請求項 1 に記載のデータ監視方法。
- 15 5. 前記複製禁止情報の更新情報は、ネットワークを介して提供されることを特徴とする請求項 4 に記載のデータ監視方法。
6. 更に、前記禁止情報記憶手段に収容された複製禁止情報を更新したときの更新履歴を保存する履歴保存処理と、前記履歴情報に基づいて更新しようとする複製禁止情報が最新の情報である場合にのみ実行される前記更新処理とを備えた請求項 1 に記載のデータ監視方法。
20
7. 前記禁止情報記憶手段に前記複製禁止情報に加えて機密管理情報を記憶しておき、当該機密管理情報とユーザの持つ機密管理レベルに基づいて複製禁止、禁止解除を制御する機密管理処理を備えた請求項 1 に記載のデータ監視方法。
8. 更に、ネットワーク上のマスタ情報記憶手段に前記複製禁止情報の原情報を収容した状態で、当該マスタ情報記憶手段に対して前記複製禁止情報の取得を要求する情報取得処理を備えた請求項 1 に記載のデータ監視方法。
25

9. 更に、上記マスタ記憶手段に前記複製禁止情報の原情報に加えて、各原情報の機密管理情報を登録しておき、前記情報取得処理において前記複製禁止情報と機密管理情報の取得をし、前記取得された機密管理情報とユーザの持つ機密管理レベルに基づいて複製禁止、禁止解除の制御をする機密管理処理とを備えた請求項 8 に記載のデータ監視方法。

10. 更に、監視機能解除権を有する者であるか否かを確認した後に、複製を停止させる機能を解除できる解除処理を備えた請求項 1 に記載のデータ監視方法。

11. 更新可能な少なくとも 1 種の複製禁止情報を収容する禁止情報記憶手段と、前記複製禁止情報に基づいて監視対象データから生成される少なくとも 1 種の複製要素を監視する監視手段と、前記少なくとも 1 種の複製要素が前記複製禁止情報の 1 つと一致すると見なされたときに前記監視対象データの入力または出力を禁止する禁止手段と、を備えたことを特徴とするデータ監視装置。

12. 更に、複製禁止情報を更新する更新手段を備えた請求項 1 に記載のデータ監視装置。

13. 前記更新手段が、前記複製禁止情報が更新権限の管理情報を属性とし、前記更新手段が更新権限を持つユーザの更新処理でない場合に更新処理に禁止をかける請求項 1 に記載のデータ監視装置。

14. 前記更新情報は、可搬記憶メディアによって提供される請求項 1 に記載のデータ監視装置。

15. 前記更新情報は、情報提供媒体によって取得される請求項 1 に記載のデータ監視装置。

16. 前記複製禁止情報がネットワークを介して取得される請求項 1 に記載のデータ監視装置。

17. 更に、前記禁止情報記憶手段の複製禁止情報を更新したときの更新履歴

を保存する履歴保存手段と、前記更新情報の履歴のに基づいて最新の複製禁止情報を取得する前記更新手段を備えた請求項 1 2 に記載のデータ監視装置。

18. 更に、禁止情報記憶手段に前記複製禁止情報に加えて機密管理情報を記憶するとともに、当該機密管理情報とユーザの持つ機密管理レベルに基づいて複製禁止、禁止解除を制御する機密管理手段を備えた請求項 1 2 に記載のデータ監視装置。
5

19. 更に、前記複製禁止情報の原情報を収容したネットワーク上のマスタ情報記憶手段と、当該マスタ情報記憶手段に対して前記複製禁止情報の取得を要求する情報取得手段を備えた請求項 1 2 に記載のデータ監視装置。

10 20. 上記マスタ記憶手段に前記複製禁止情報の原情報を加えて、各原情報の機密管理情報を登録するとともに、前記情報取得手段が前記複製禁止情報と機密管理情報の取得するようにし、更に、前記取得された機密管理情報とユーザの持つ機密管理レベルに基づいて複製禁止、禁止解除の制御をする機密管手段を備えた請求項 1 9 に記載のデータ監視装置。

15 21. 更に、監視機能解除権を有する者であるか否かを確認した後に、複製を停止させる機能を解除できる解除手段を備えた請求項 1 2 に記載のデータ監視装置。

22. 監視対象データの生成に関与した所定の装置に固有な識別情報を抽出する第 1 の特定情報抽出手段と、前記監視対象データに前記識別情報を付与し、
20 新たな複製データを生成する情報付加手段と、を備えたことを特徴とする複製装置。

23. 前記識別情報は中央処理装置 (C P U) に付与されたチップ識別情報である請求項 2 2 に記載の複製装置。

24. 前記識別情報は装置に付与された I P アドレスである請求項 2 2 に記載
25 の複製装置。

25. 複製監視対象データの生成に関与したソフトウェアに固有な特定アプリケーション情報を抽出する第2の特定情報抽出手段と、前記監視対象データに前記特定アプリケーション情報を付与し、新たな複製データを生成する情報付加手段と、を備えたことを特徴とする複製装置。

5 26. 前記特定アプリケーション情報は、ユーザが設定しているメールアドレスである請求項25に記載の複製装置。

27. 外部機器より監視対象データを受け入れ、当該監視対象データに従って複製物を生成する複製装置において、前記監視対象データを解析し、該監視対象データに関与した所定の装置を特定する固有情報を抽出する抽出手段と、抽出した固有情報を前記監視対象データ付与する特定情報付与手段と、を備えた複製装置。

10 28. 前記固有情報とは、パーソナルコンピュータを特定できる識別番号である請求項27に記載の複製装置。

15 29. 前記識別情報は装置に付与されたIPアドレスである請求項28に記載の複製装置。

30. 外部機器より監視対象データを受け入れ、前記監視対象データに従って複製物を生成する複製装置において、前記複製データを解析し、複製データに関与したソフトウェアを特定する固有情報を抽出する抽出手段と、抽出した固有情報を新たな複製データとして複製物に付与する特定情報付与手段と、を備えたことを特徴とする複製装置。

20 31. 前記固有情報は、ユーザが設定しているメールアドレスである請求項30に記載の複製装置。

32. 前記固有情報は、ソフトウェアの登録情報である請求項30に記載の複製装置。

25 33. 外部機器より監視対象データを受け入れ、前記監視対象データに従って

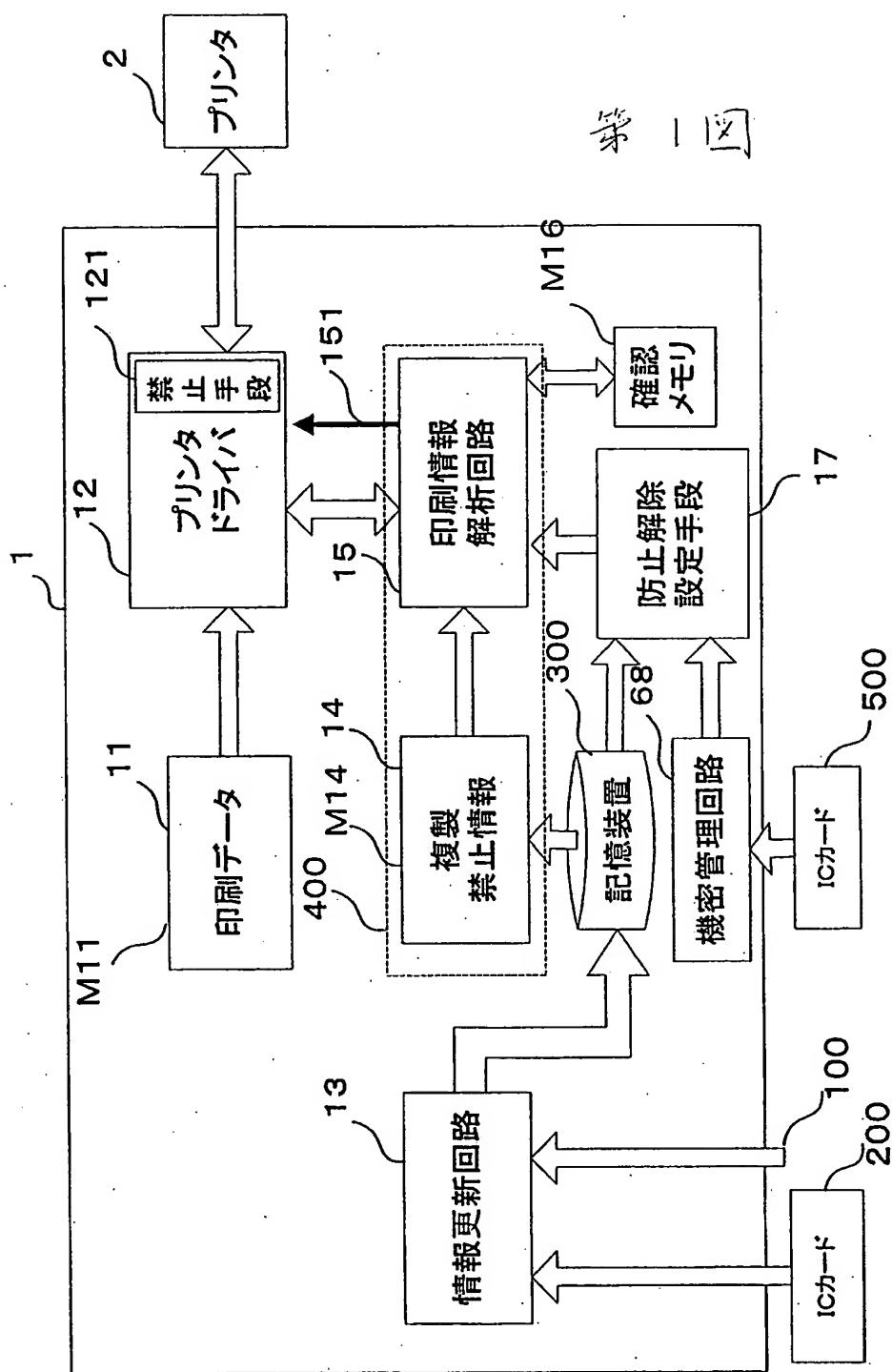
複製物を生成するネットワーク対応の複製装置において、前記複製装置に付与されたIPアドレスを抽出する抽出手段と、抽出したIPアドレスを新たな複製データとして複製物に付与する特定情報付与手段と、を備えたことを特徴とする複製装置。

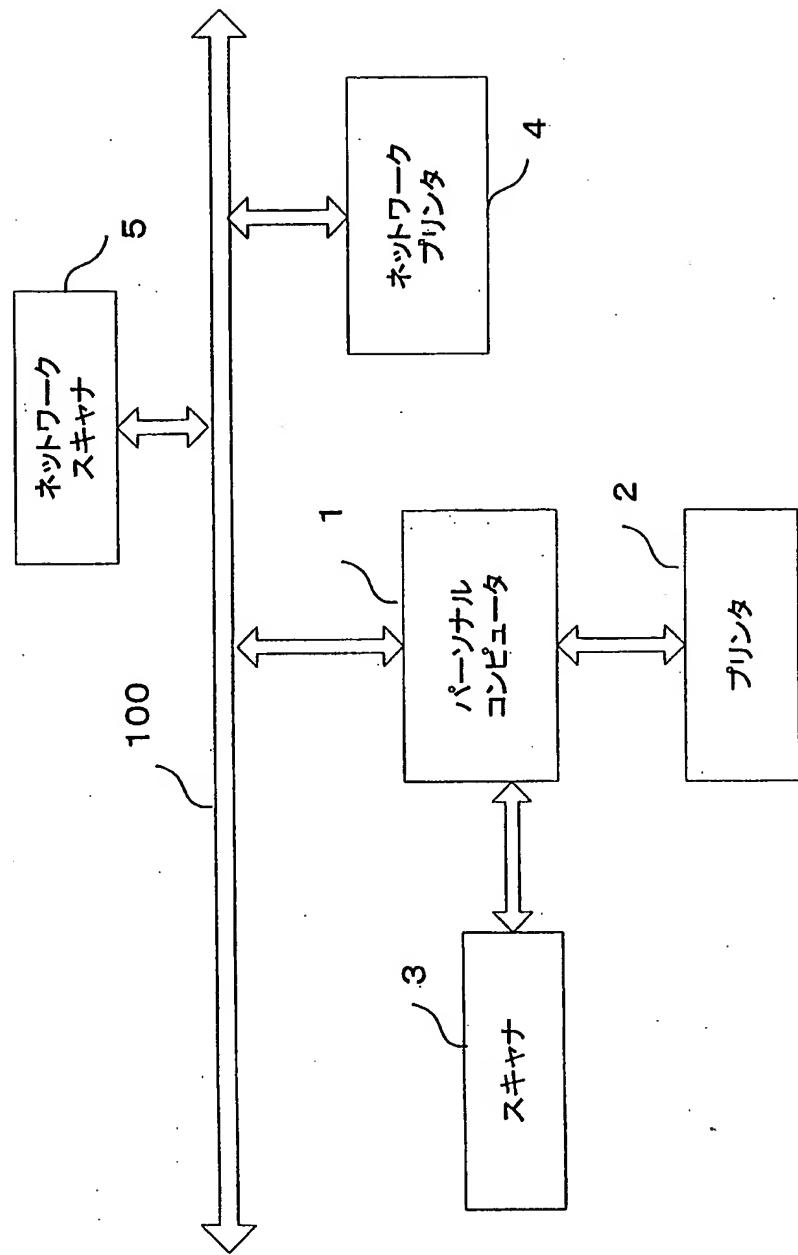
5 34. 禁止情報記憶手段に収容されるとともに更新可能な少なくとも1種の複製禁止情報に基づいて、少なくとも1種の複製要素より構成される監視対象データの各複製要素を監視する監視処理と、前記監視処理によって、前記各複製要素が前記複製禁止情報の1種と一致すると見なされたときに監視対象データの入力または出力を禁止する禁止処理とをプログラムとして記憶した記憶媒体。

10 35. 前記禁止情報記憶手段に前記複製禁止情報に加えて機密管理情報を記憶しておき、当該機密管理情報をユーザの持つ機密管理レベルとに基づいて複製禁止、禁止解除を制御する機密管理処理をプログラムとして記憶した記憶媒体。

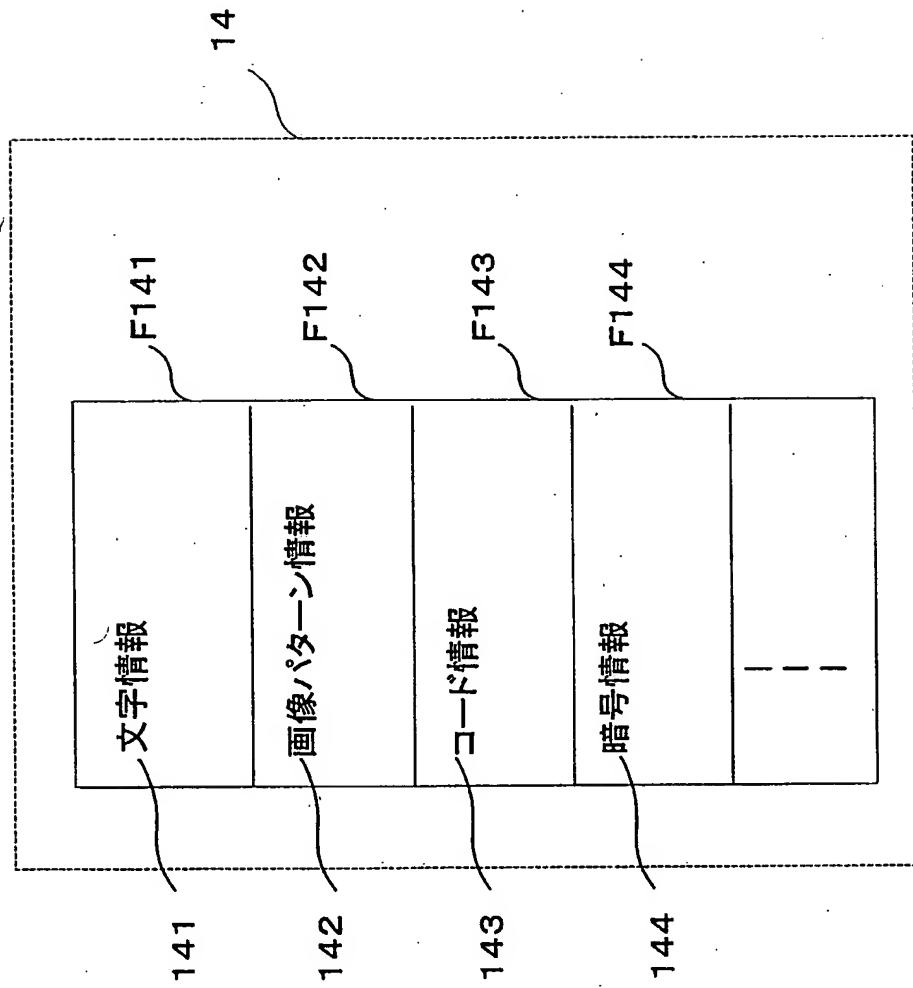
36. 外部機器より監視対象データを受け入れ、あるいは自ら監視対象データを生成して、当該監視対象データに従って複製物を生成する複製装置において、監視対象データの生成に関与した所定の装置に固有な識別情報を抽出する第1の特定情報抽出処理と、前記監視対象データに前記識別情報を付与し、新たな複製データを生成する情報付加処理とをプログラムとして記憶する記憶媒体。

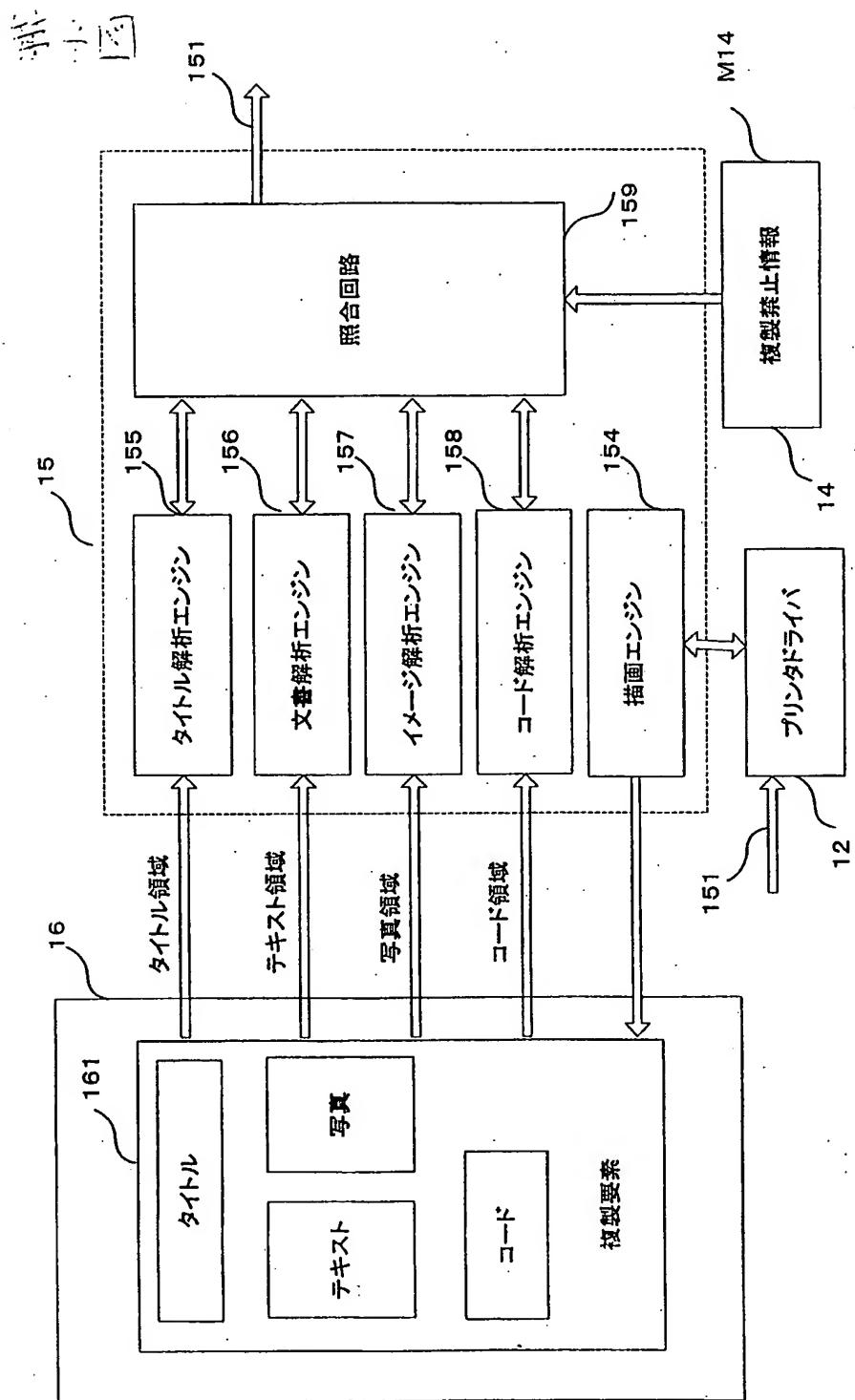
15 37. 外部機器より監視対象データを受け入れ、あるいは自ら監視対象データを生成して、当該監視対象データに従って複製物を生成する複製装置において、複製監視対象データの生成に関与したソフトウェアに固有な特定アプリケーション情報を抽出する第2の特定情報抽出処理と、前記監視対象データに前記特定アプリケーション情報を付与し、新たな複製データを生成する情報付加処理とをプログラムと記憶する。

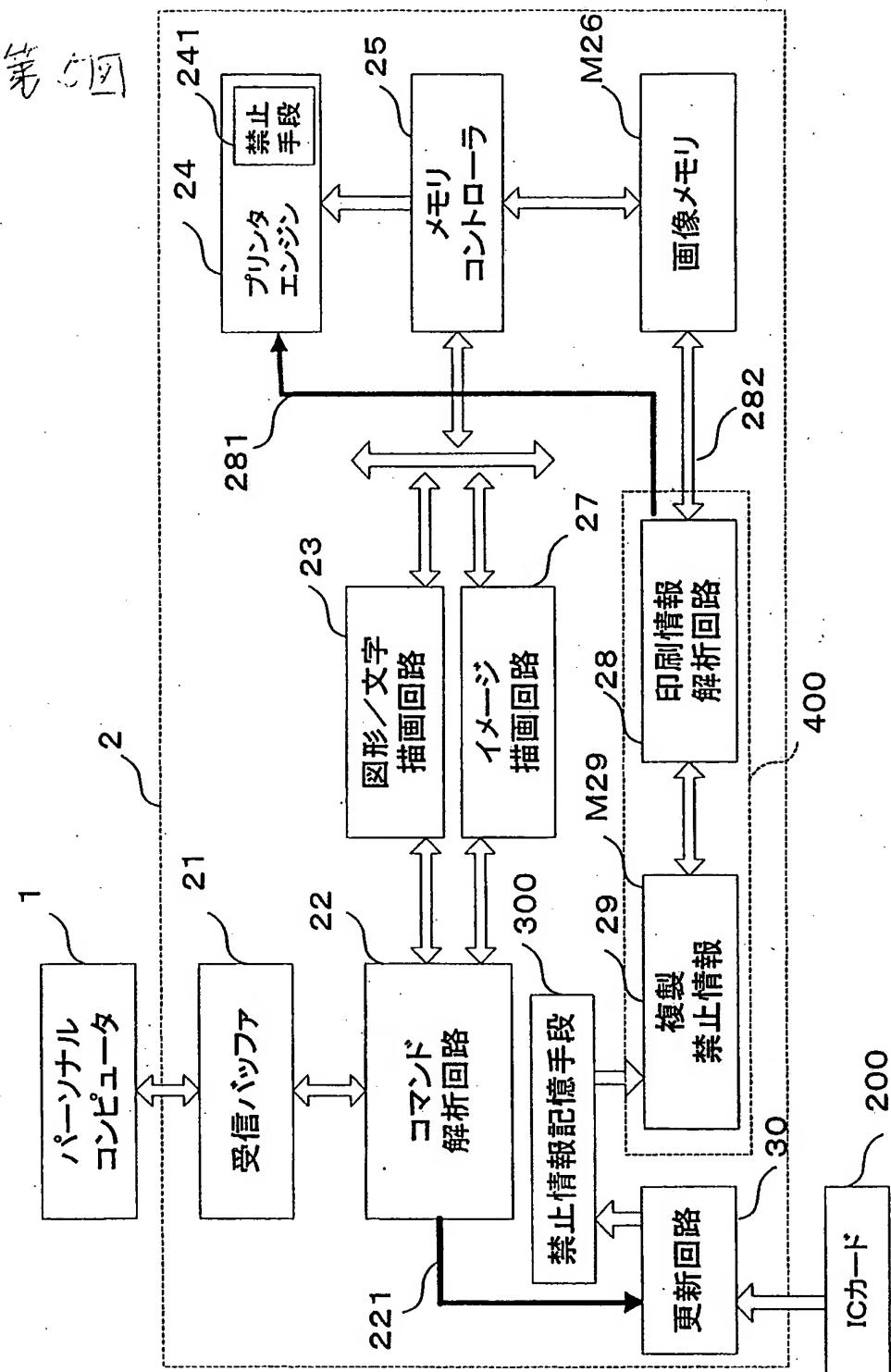


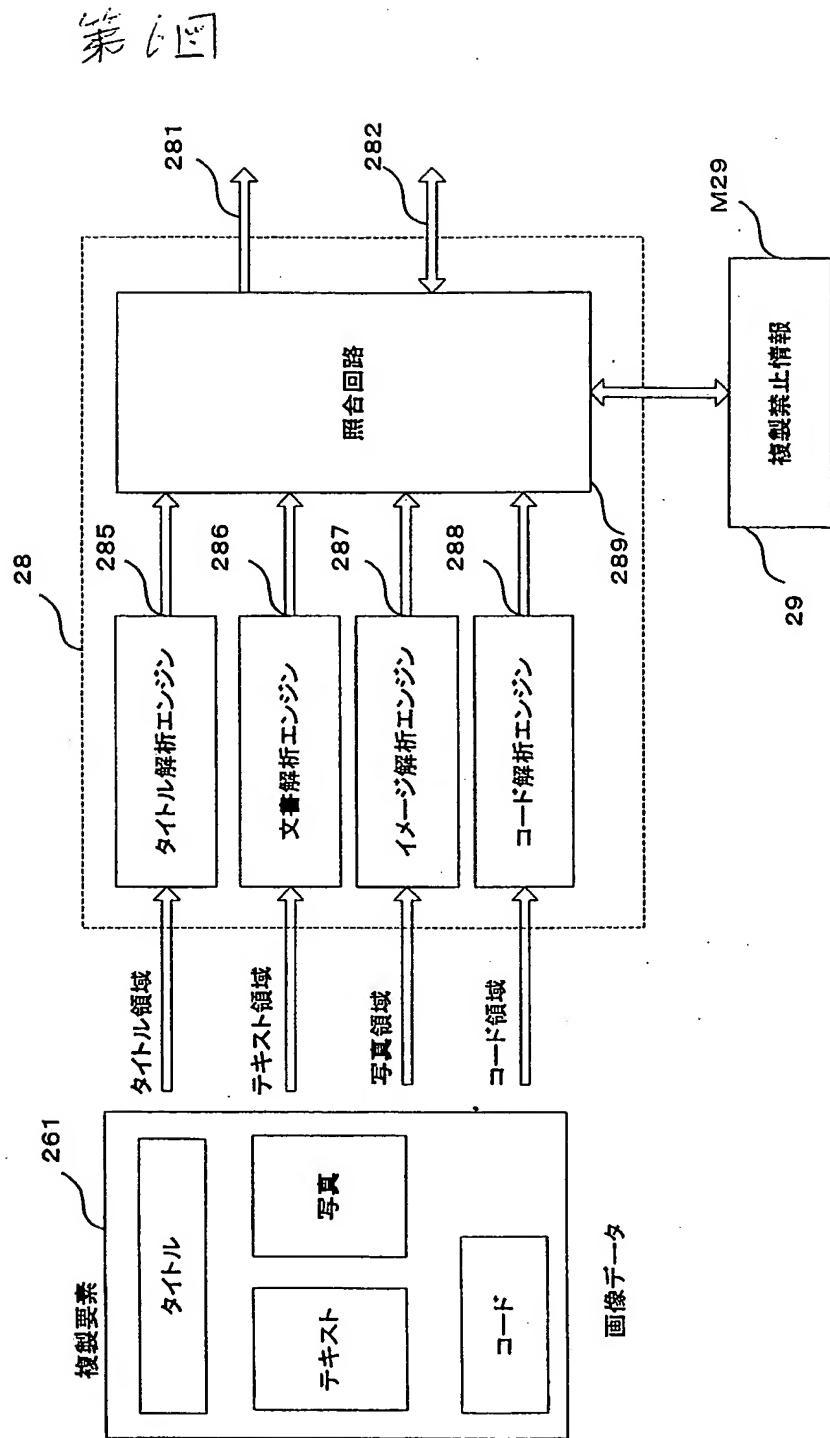
手本
1
2

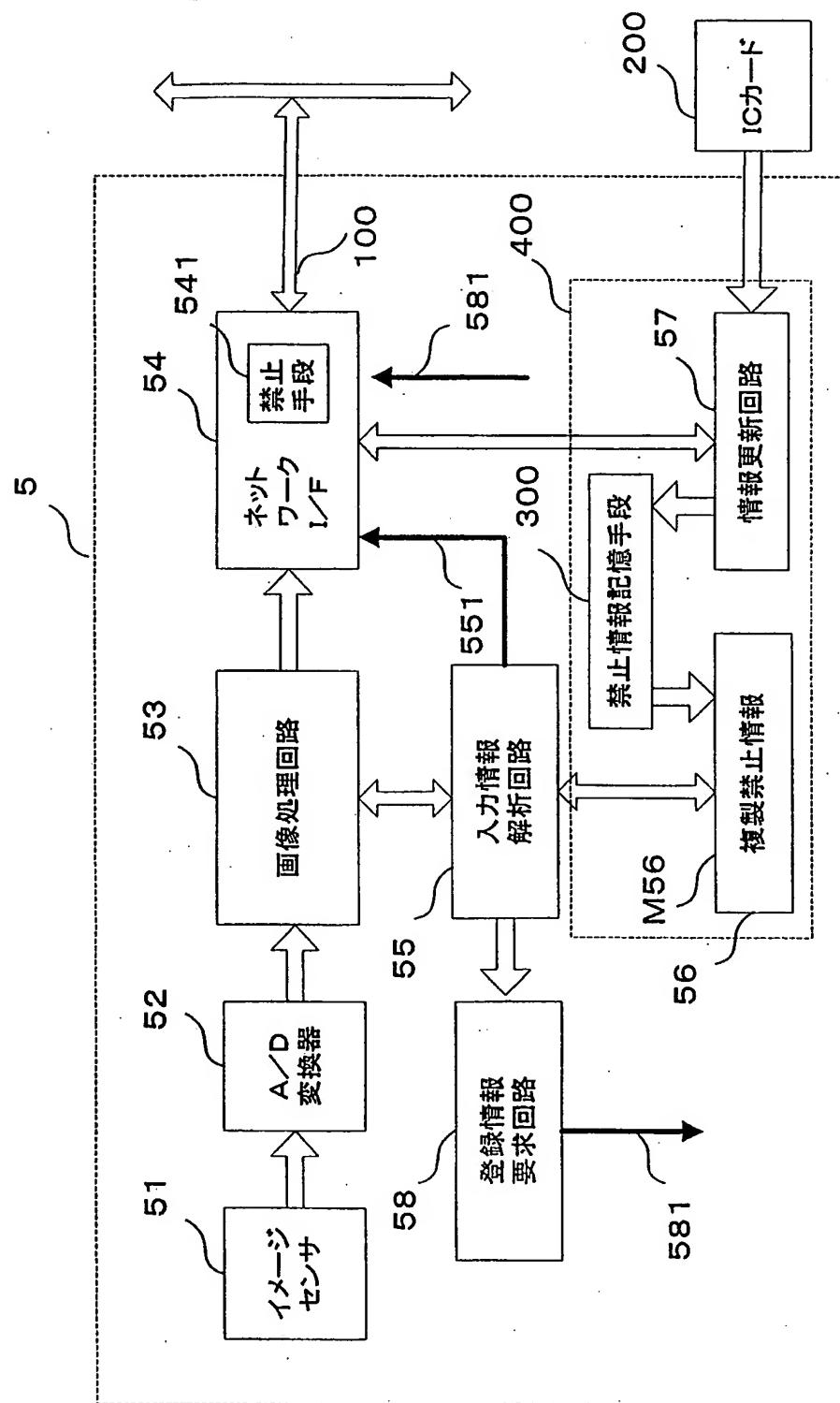
312

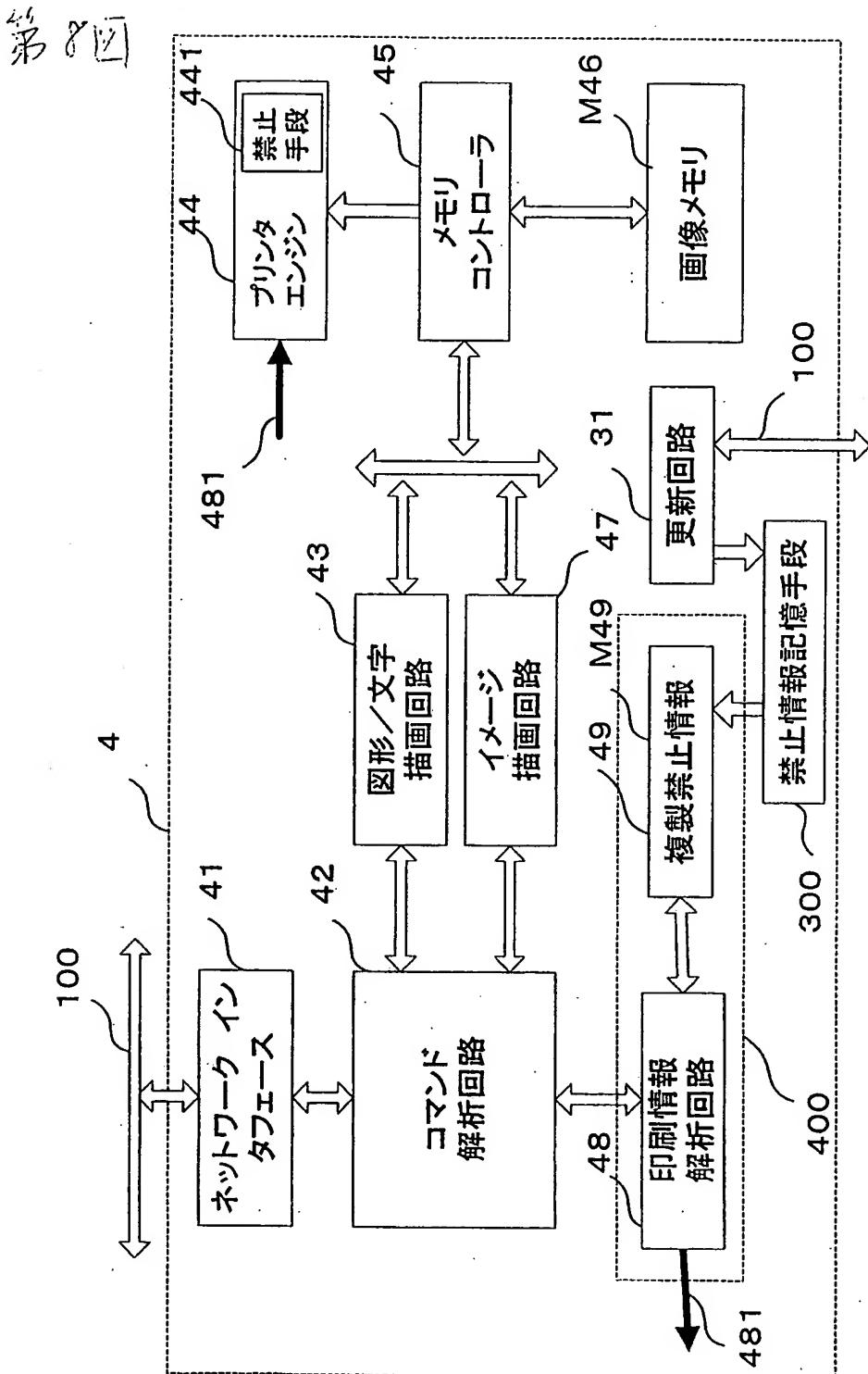


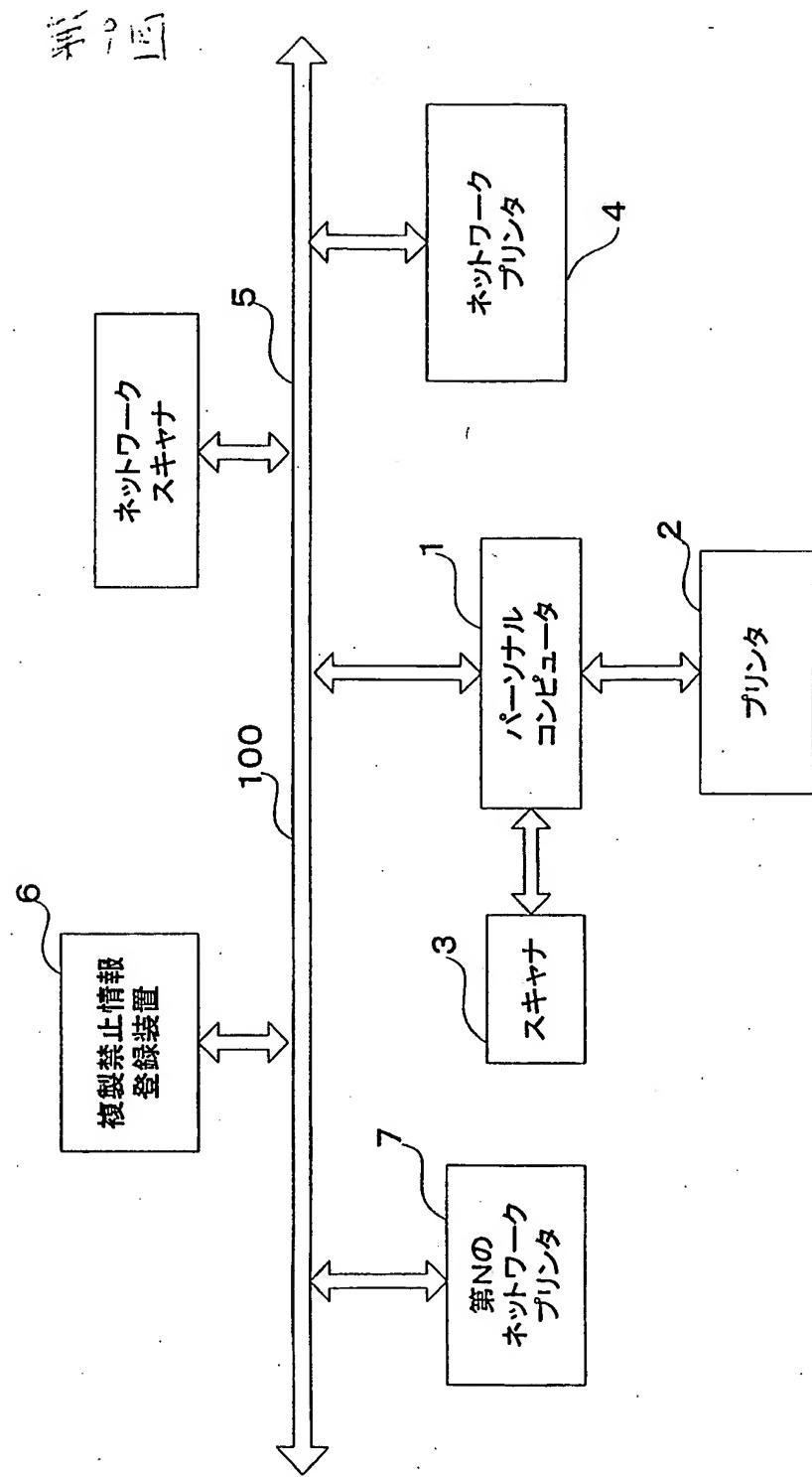


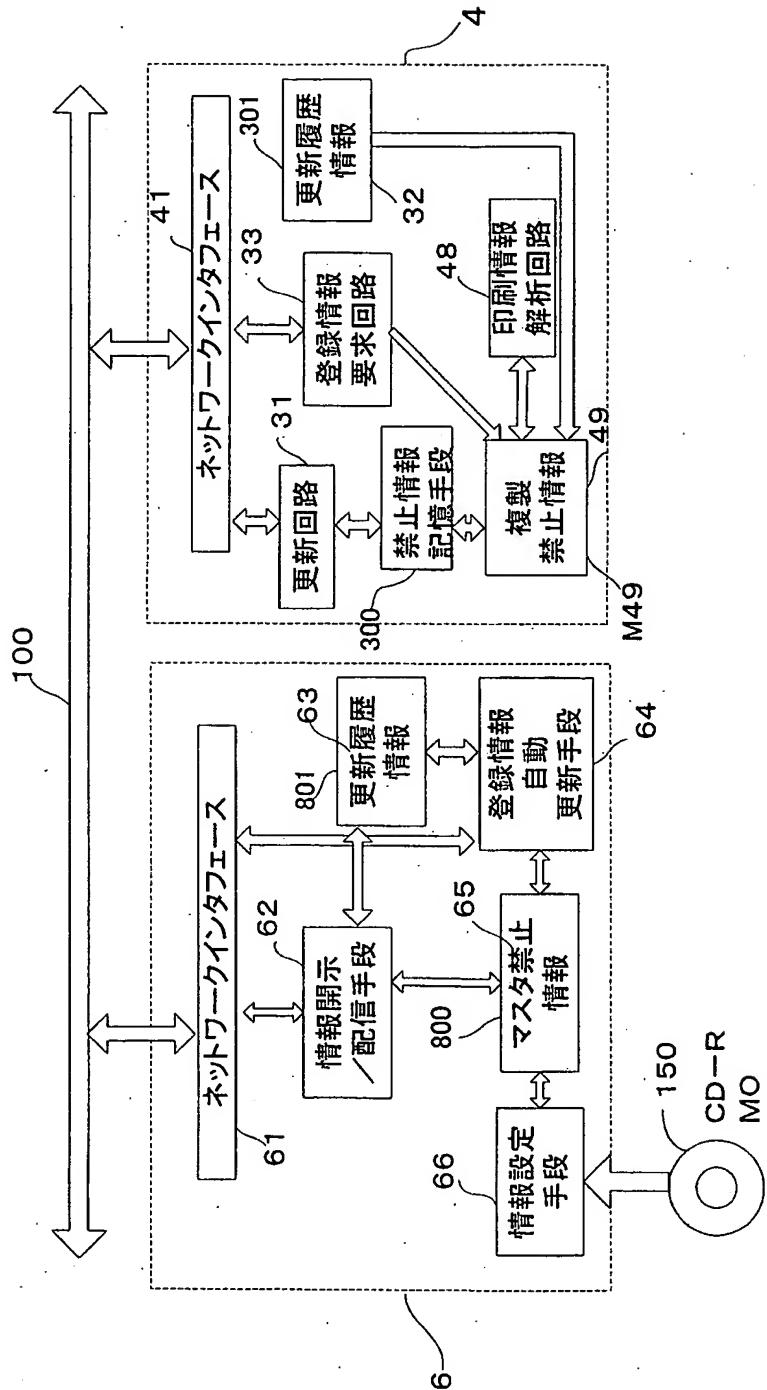


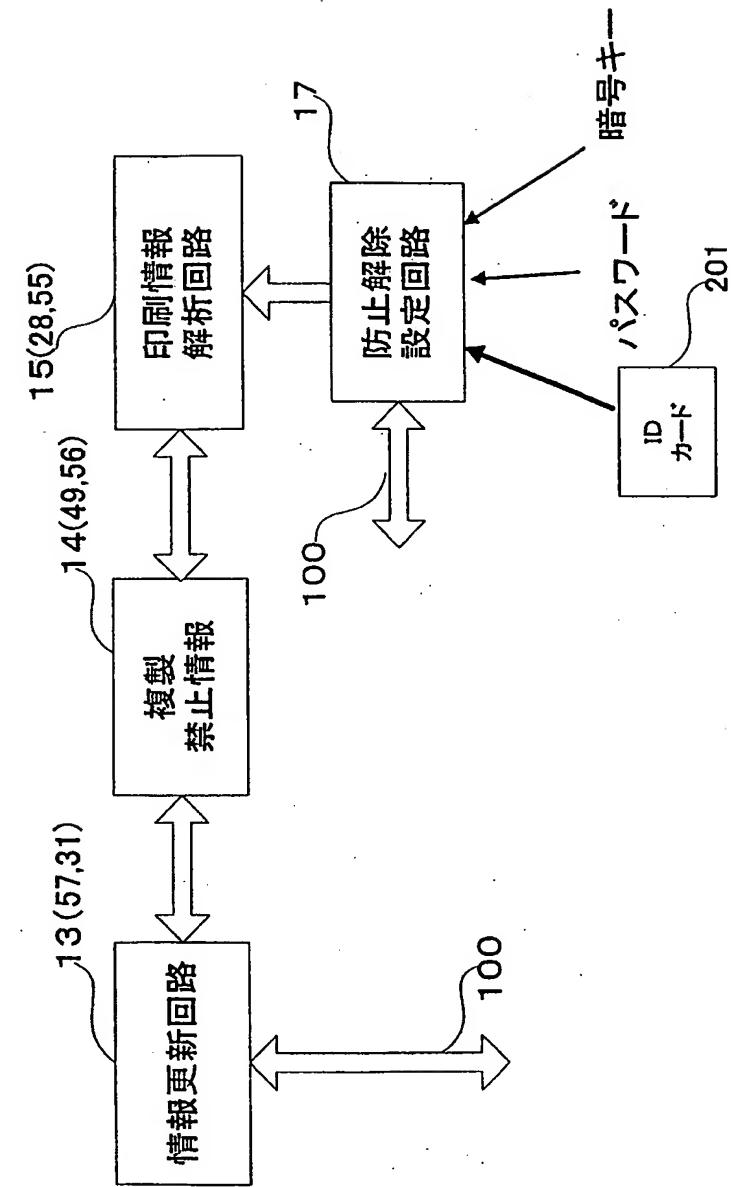




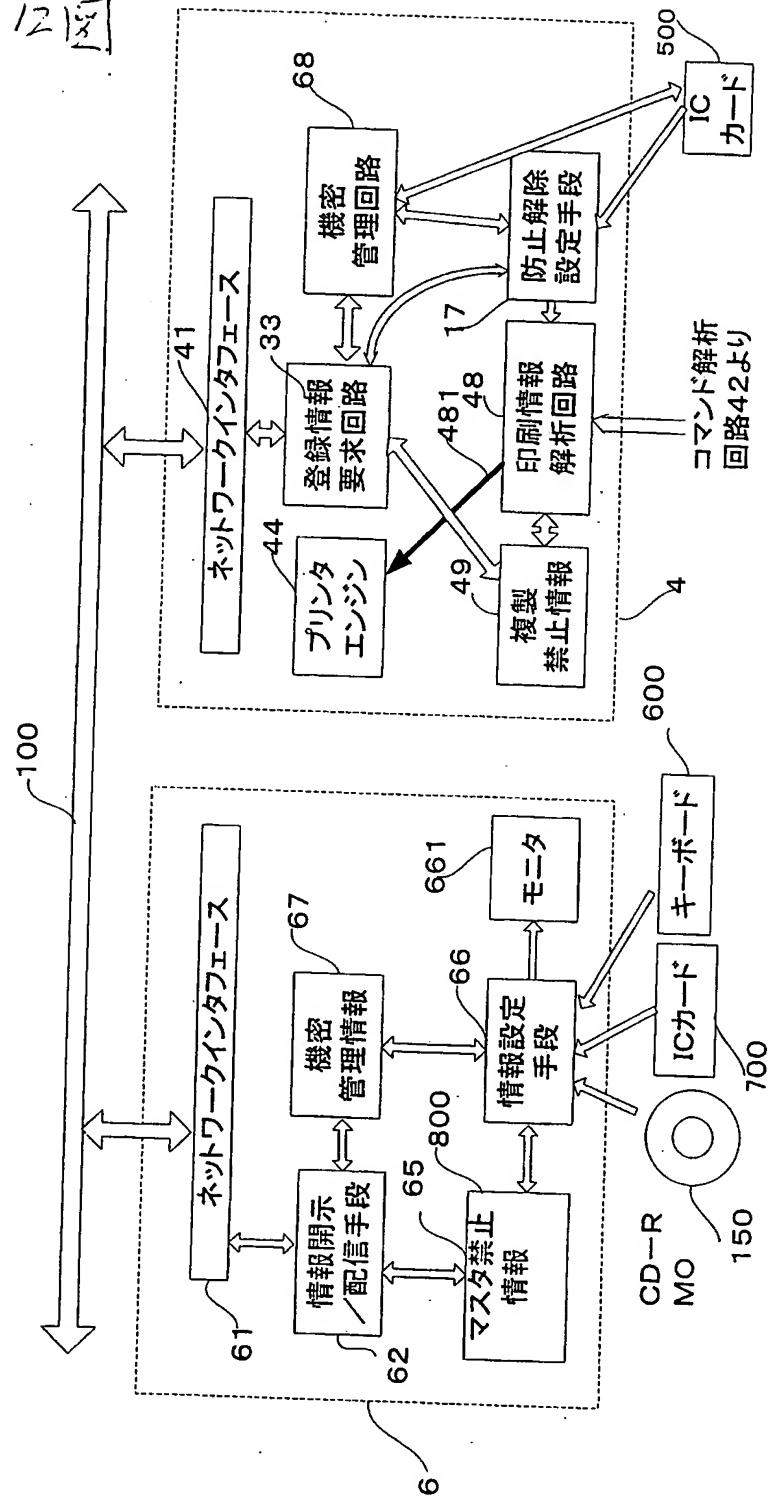








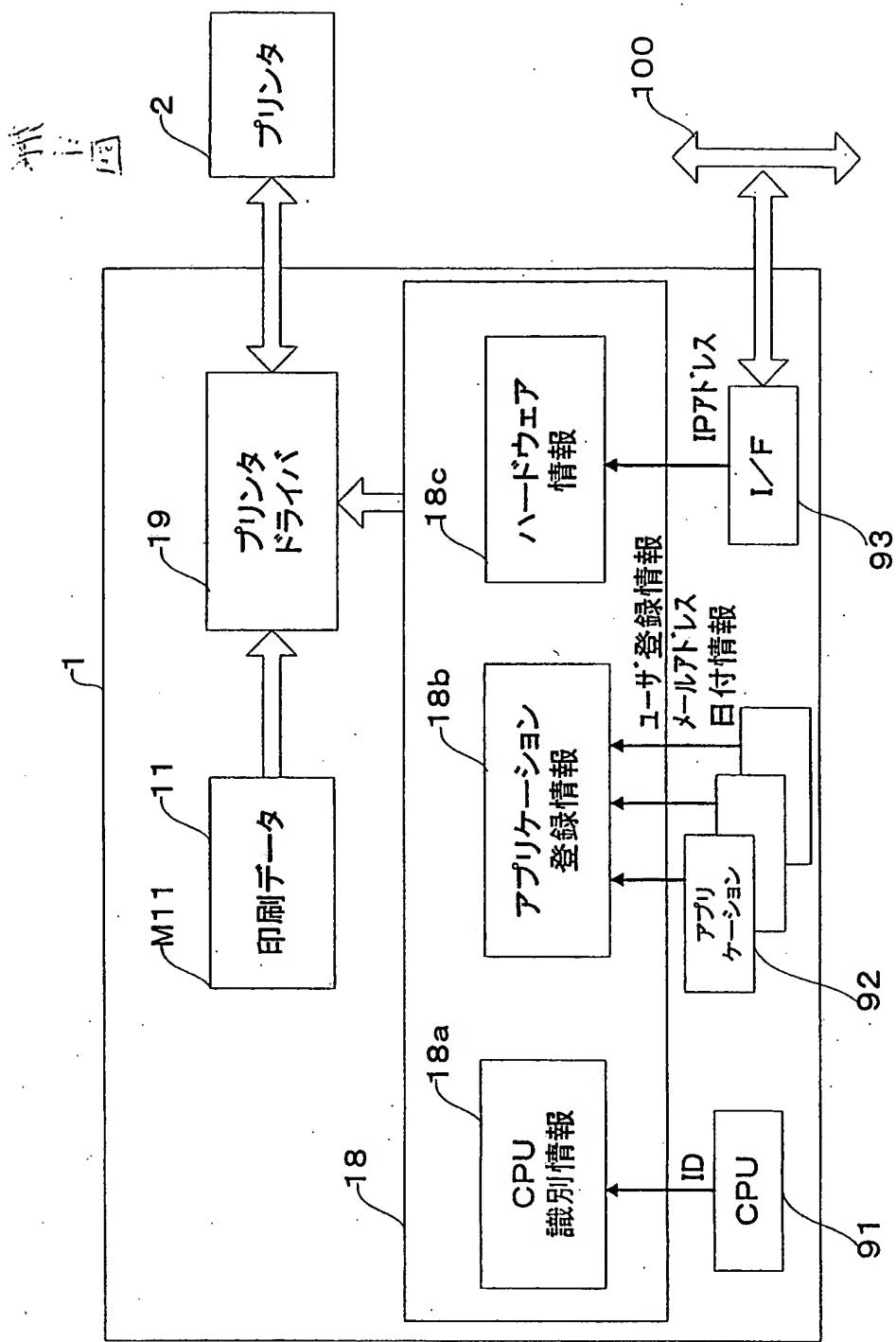
第12回

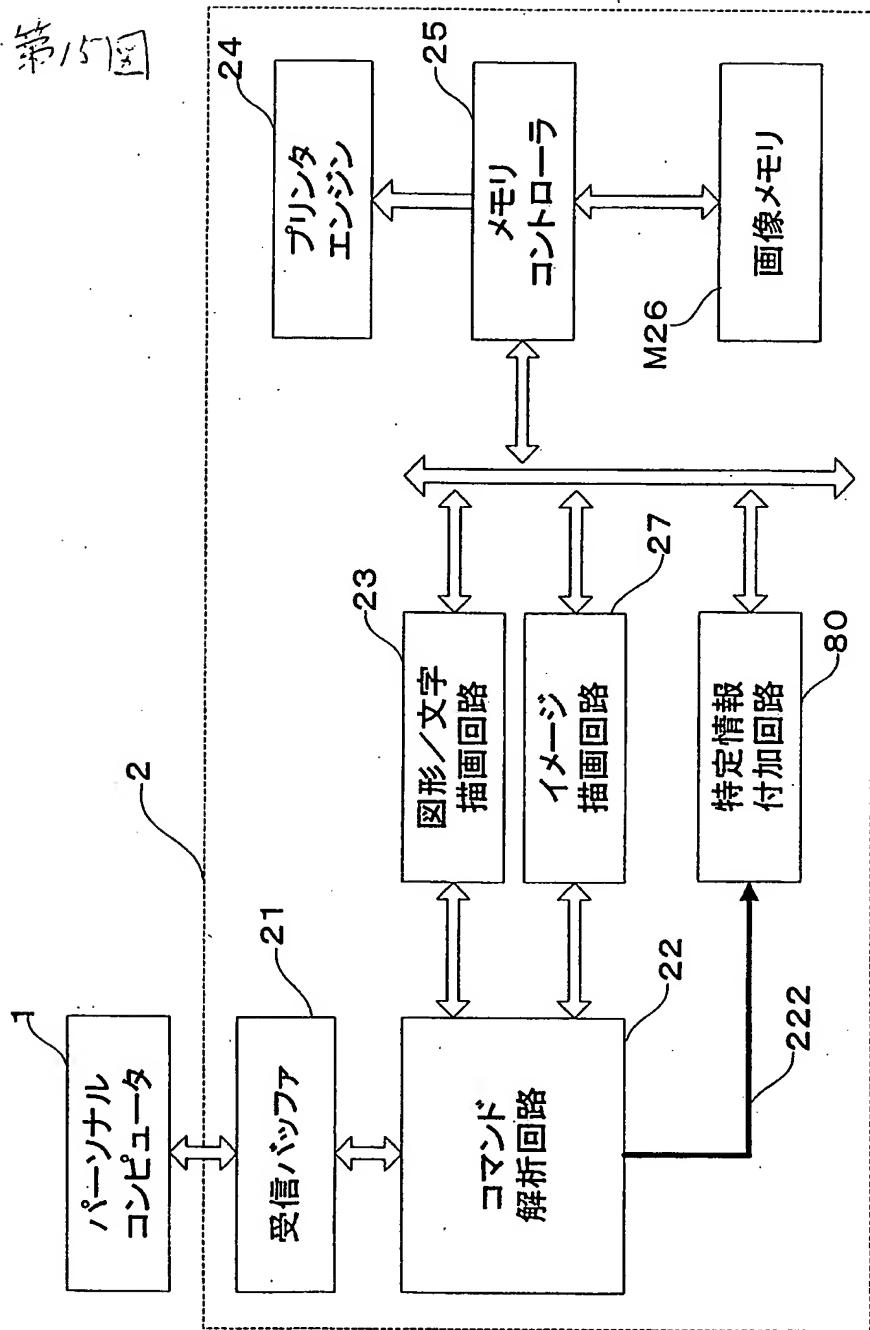


第15回

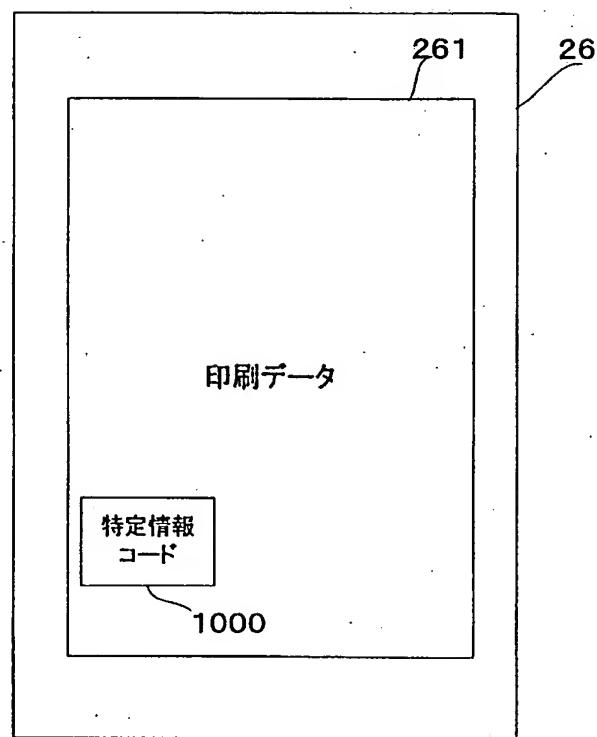
670

情報ID	許可レベル	所属ID	個人ID
D001	A001	X00	ID1／PW1
D002	B001	X00	
D003	C001	X00	
D004	C002	Y00	ID1／PW1
D005	B002	Z00	
D006	A002	A00	ID1／PW1
:	:	:	:
Dnnn	P_1n1	Gnn	IDn／PWn

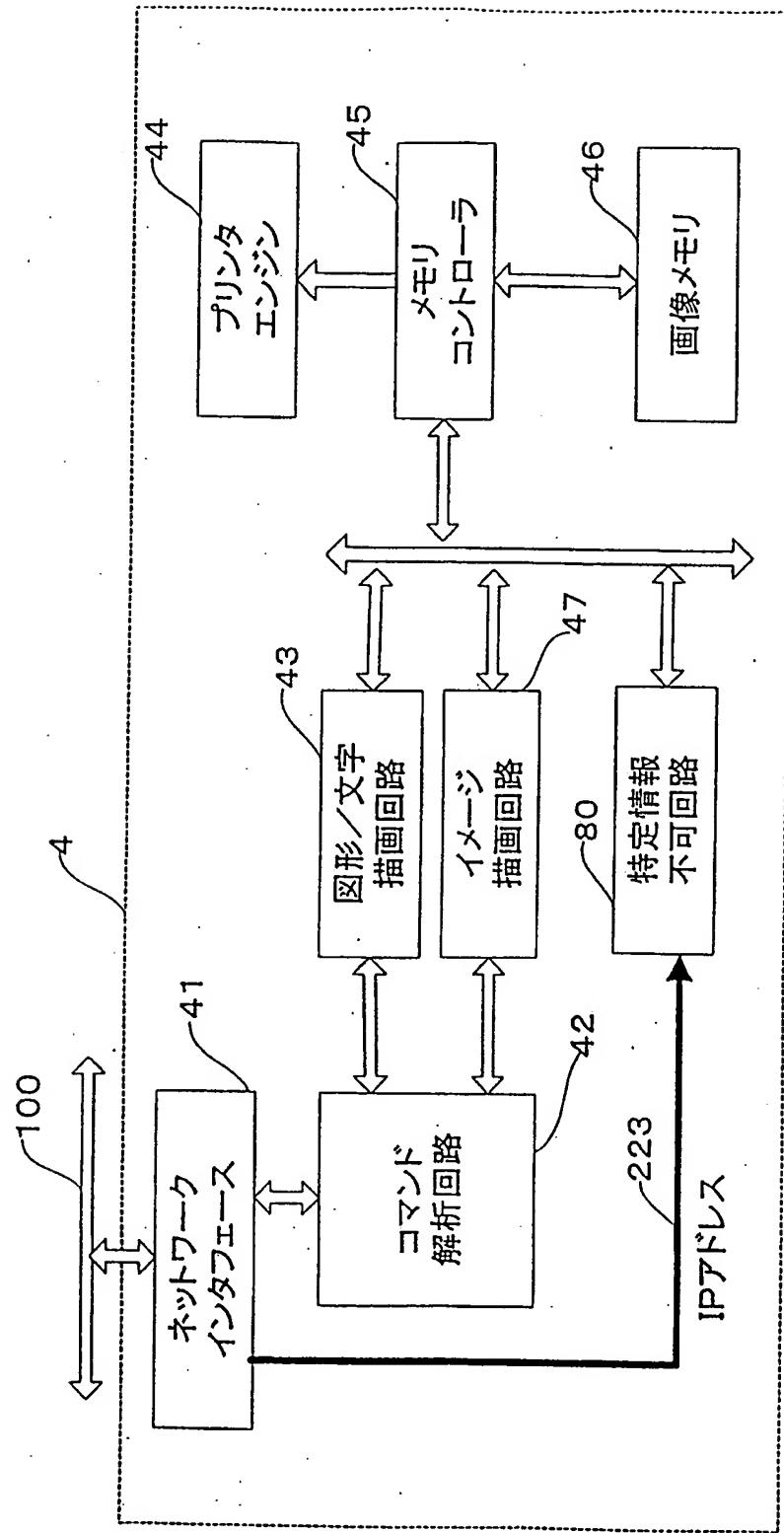




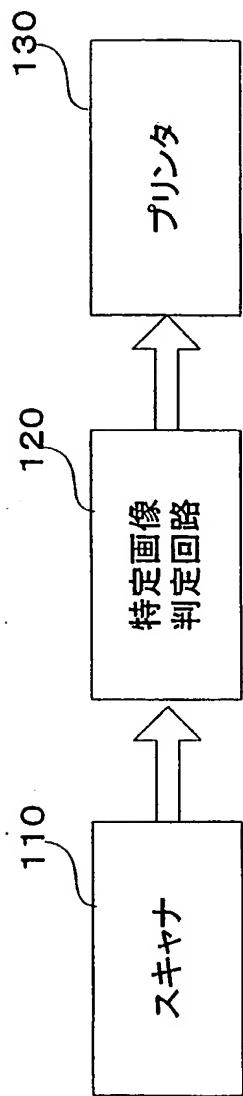
第16図



第17回



第18回



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/01097

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. 7 H04N 1/40, H04N 1/387

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int. Cl. 7 H04N 1/40-1/409, H04N 1/46, H04N 1/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1926-1996	Jitsuyo Shinan Toroku Koho	1996-2000
Kokai Jitsuyo Shinan Koho	1971-2000	Toroku Jitsuyo Shinan Koho	1994-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	J P, 6-178066, A (Minolta Camera Co., LTD.) 24. June. 1994 (24. 06. 94), Full text (Family: none)	1, 2, 4-6, 8, 11-13, 15, 16, 19, 22-24, 27-29, 33, 34, 36
Y		7, 9, 17, 18, 20, 25, 26, 30-32, 35, 37
X	J P, 5-282448, A (Canon Inc.) 29. October. 1993 (29. 10. 93), Full text (Family: none)	1-5, 11-16, 19, 34, 35
Y		7, 9, 18, 20
X	J P, 3-120561, A (Canon Inc.) 22. May. 1991 (22. 05. 91), Full text (Family: none)	1-4, 10-15, 21, 34

Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:	
"A"	document defining the general state of the art which is not considered to be of particular relevance
"B"	earlier document but published on or after the international filing date
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O"	document referring to an oral disclosure, use, exhibition or other means
"P"	document published prior to the international filing date but later than the priority date claimed
"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&"	document member of the same patent family

Date of the actual completion of the international search 23 May, 2000 (23.05.00)	Date of mailing of the international search report 06.06.00
--	--

Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/01097

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP, 5-14706, A (Canon Inc.) 22. January. 1993 (22. 01. 93), Full text (Family: none)	1-5, 11-16
X	JP, 3-139974, A (Canon Inc.) 14. June. 1991 (14. 06. 91), Full text (Family: none)	1-4, 11-15, 34
Y		7, 18
X	JP, 6-125459, A (Ricoh Company Ltd.) 6. May. 1994 (06. 05. 94), Full text	22-24, 36
Y	&WO, 94/09590, A1	7, 9, 18, 20, 35
X	JP, 6-70134, A (Ricoh Company Ltd.) 11. March. 1994 (11. 03. 94), Full text	22-24
	&WO, 94/03996, A1	
	&GB, 2277223, A	
Y	WO, 95/01043, A1 (Omron Corporation) 5. January. 1995 (05. 01. 95), Full text (Family: none)	7, 9, 18, 20
Y	JP, 2-73284, A (Canon Inc.) 13. March. 1990 (13. 03. 90), Full text (Family: none)	7, 9, 18, 20
Y	JP, 6-70150, A (Ricoh Company Ltd.) 11. March. 1994 (11. 03. 94), Full text (Family: none)	10, 21

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl. 7 H04N1/40, H04N1/387

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl. 7 H04N1/40-1/409, H04N1/46, H04N1/60

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996年

日本国公開実用新案公報 1971-2000年

日本国実用新案登録公報 1996-2000年

日本国登録実用新案公報 1994-2000年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリーエ	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP, 6-178066, A (ミノルタカメラ株式会社) 24. 6 月. 1994 (24. 06. 94), 全文 (ファミリーなし)	1, 2, 4-6, 8, 11-13, 15, 16, 19, 22-24, 27- 29, 33, 34, 36 7, 9, 17, 18, 20, 25, 26, 30- 32, 35, 37
Y		
X	JP, 5-282448, A (キャノン株式会社) 29. 10月. 1993 (29. 10. 93), 全文 (ファミリーなし)	1-5, 11-16, 19, 34, 35 7, 9, 18, 20
Y		

 C欄の続きにも文献が列挙されている。 パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリーエ

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

23. 05. 00

国際調査報告の発送日 06.06.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

田 中 純 一

5V 9074

電話番号 03-3581-1101 内線 3571

C (続き) 関連すると認められる文献		関連する請求の範囲の番号
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	
X	JP, 3-120561, A (キャノン株式会社) 22. 5月. 1991 (22. 05. 91), 全文 (ファミリーなし)	1-4, 10-15, 21, 34
X	JP, 5-14706, A (キャノン株式会社) 22. 1月. 1993 (22. 01. 93), 全文 (ファミリーなし)	1-5, 11-16
X	JP, 3-139974, A (キャノン株式会社) 14. 6月. 1991 (14. 06. 91), 全文 (ファミリーなし)	1-4, 11-15, 34
Y		7, 18
X	JP, 6-125459, A (株式会社リコー) 6. 5月. 1994 (06. 05. 94), 全文&WO, 94/09590, A1	22-24, 36
Y		7, 9, 18, 20, 35
X	JP, 6-70134, A (株式会社リコー) 11. 3月. 1994 (11. 03. 94), 全文&WO, 94/03996, A1&GB, 2277223, A	22-24
Y	WO, 95/01043, A1 (オムロン株式会社) 5. 1月. 1995 (05. 01. 95), 全文 (ファミリーなし)	7, 9, 18, 20
Y	JP, 2-73284, A (キャノン株式会社) 13. 3月. 1990 (13. 03. 90), 全文 (ファミリーなし)	7, 9, 18, 20
Y	JP, 6-70150, A (株式会社リコー) 11. 3月. 1994 (11. 03. 94), 全文 (ファミリーなし)	10, 21